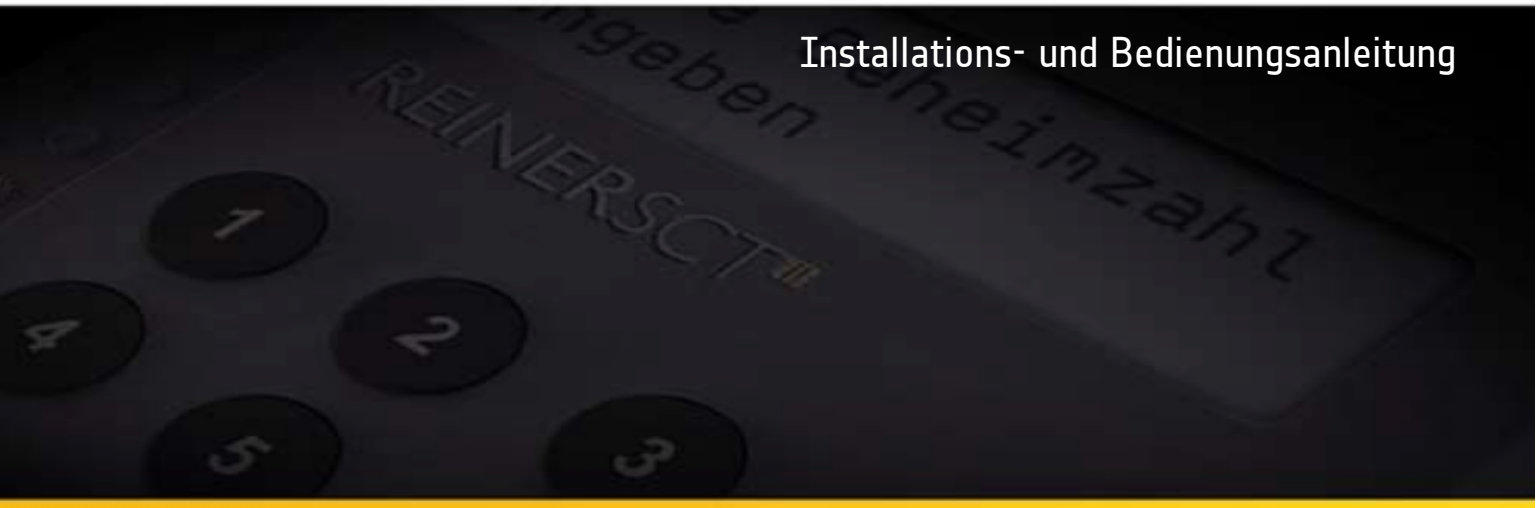
REINERSCT

cyber*Jack*®



Installations- und Bedienungsanleitung

Inhaltsverzeichnis

1 Vorwort 1

2 Gerätebeschreibung 2

3 Chipkartenleser in Betrieb nehmen 5

3.1 Chipkartenleser auspacken und aufstellen 5
3.2 Beschreibung der Bedienelemente 6
3.3 Maßnahmen zum sicheren Betrieb 7

4 Installation der Hardware am PC 8

4.1 cyberJack USB 8
4.2 cyberJack TWIN seriell 9
4.3 cyberJack LPT 10

5 Installation der Softwarekomponente 11

6 Die Funktionen Ihres Chipkartenlesers 13

6.1 Gerätemanager 13
6.2 Die Funktion sichere PIN-Eingabe 17
6.3 Integration des cyberJack-Chipkartenlesers in Anwendungen 18
6.4 TAN-Generierung nach HHD 1.3 18

7 Modulverwaltung 21

8 cyberJack biometric 22

8.1 Menü 23
8.2 Erfassen 24
8.3 Ändern 25
8.4 Löschen 26
8.5 Selbsttest 26

9 Support 27

10 Windows Terminal Server und CITRIX Administrator Guide 28

11 Technische Referenzen 36

11.1 LED-Funktionen 36
11.2 Geräteidentifizierung 37
11.3 Sicherheitsfunktionen 38

12 Sicherheitshinweise 39

13 Konformitätserklärungen 40

13.1 cyberJack pinpad 40
13.2 cyberJack secoder 41

13.3 cyberJack ecom 42
13.4 cyberJack e-com plus 43
14 SigG-Bestätigungen 44
14.1 cyberJack secoder 44
14.2 cyberJack e-com 48
14.3 cyberJack e-com plus 52
Index 56

1 Vorwort

Liebe Kundin, lieber Kunde,

vielen Dank, dass Sie sich für einen Chipkartenleser aus der cyber***Jack***® Familie von **REINER**SCT entschieden haben. Das Gerät wurde in Deutschland entwickelt und mit größter Sorgfalt hergestellt, so dass es Sie viele Jahre zuverlässig unterstützt. Nachfolgend möchten wir Sie kurz über die wichtigsten Einsatzgebiete eines cyber***Jack***® Chipkartenlesers informieren.

HBCI – Homebanking*

Kontoabfragen, Überweisungen und Wertpapiergeschäfte von zu Hause aus tätigen: Die Basis für sicheres Homebanking ist HBCI. Dieser Standard der deutschen Kreditwirtschaft ist dem Verfahren mit PIN und TAN weit überlegen. Denn HBCI bietet deutlich mehr Sicherheit und Komfort:
Daten, die über das Internet an die Bank geschickt werden, werden zuvor verschlüsselt und mit einer elektronischen Signatur versehen.

Elektronische Signatur – Die Unterschrift fürs Internet*

Die rechtsgültige persönliche Unterschrift im Internet kommt und mit ihr der Schutz vor Manipulation: die Elektronische Signatur. Mit dieser elektronischen Unterschrift können Sie Verträge, Steuererklärungen, Dokumente an kommunale Dienste aber auch E-Mails und vieles mehr signieren und verschlüsseln.

* Für diese Anwendungen benötigen Sie ggf. noch Zusatzsoftware und/oder Chipkarten von Drittanbietern. Homebanking-Chipkarten erhalten Sie von Ihrem Kreditinstitut, Signaturkarten von Trustcentern.

GeldKarte – Sicher bezahlen im Internet

Geld elektronisch bei der Bank holen und damit im Internet bezahlen. Die GeldKarte gewährleistet Ihnen dabei absolute Anonymität und höchste Sicherheit.

Biometrie – Endlich keine PIN mehr merken

Einfach den Finger kurz auflegen und schon steht der Zugang zu Computer und Konto offen. Aufwand, Kosten und Ärger durch vergessene PINs und Passwörter gehören der Vergangenheit an.

Mit der cyber***Jack***®-Produktfamilie finden Sie für alle diese Anwendungen das passende Gerät. Wie Sie Ihren Chipkartenleser anschließen, bedienen und in Ihre Anwendungen integrieren, beschreibt die vorliegende Anleitung.

Viel Erfolg mit Ihrem neuen Gerät wünscht Ihnen

REINER SCT
Reiner Kartengeräte GmbH & Co. KG
Goethestraße 14
78120 Furtwangen
Germany

www.reiner-sct.com

2 Gerätebeschreibung

cyber*Jack*® pinpad

Mit dem cyber***Jack***® **pinpad** sind sensible Daten wie die Karten-PIN vor Hackern sicher: Das Gerät erfüllt die Anforderungen der Sicherheitsklasse 2 für Chipkartenlesegeräte. Bei der Eingabe werden die PIN-Daten über die Gerätetastatur direkt an die Chipkarte weitergegeben – ohne Umweg über den PC. So können sie nicht durch Viren oder ein trojanisches Pferd ausgespäht werden.
Das Gerät lässt sich mit einem abnehmbaren Metall-Standbügel in ergonomischer Pultform aufstellen und kann ohne Standfuß platzsparend untergebracht werden, z.B. in der Notebooktasche.

cyberJack® pinpad

cyber*Jack*® e-com

Der cyber***Jack***® **e-com** ist ein Chipkartenleser der Sicherheitsklasse 3. Zusätzlich zu den Funktionen Homebanking und elektronische Signatur kann man mit diesem Gerät auch im Internet mit der GeldKarte bezahlen. Außerdem kann die Gerätefirmware des cyber***Jack***® **e-com** aktualisiert werden und weitere Applikationen sind nachladbar, was das Gerät sehr zukunftsfähig macht.

cyberJack® e-com

cyber*Jack*® biometric

Der cyber***Jack***® **biometric** basiert auf dem cyber***Jack***® **e-com** der um ein Zusatzmodul zum Erfassen und Erkennen von Fingerabdrücken erweitert wurde. Alle für den cyber***Jack***® **e-com** beschriebenen Funktionen gelten auch für den cyber***Jack***® **biometric** entsprechend.

cyberJack® biometric

cyber*Jack*® e-com plus

Der neue cyber***Jack***® **e-com plus** mit seinem unverwechselbaren und frischen Design besitzt ein großes LC-Display mit dezenter Hintergrundbeleuchtung. Die hochwertigen und griffigen Tasten, den äußerst stabilen Metallstandfuß und die angenehme, ergonomische Bedienposition machen ihn zum Highlight der cyber***Jack***® Familie. Als Weiterentwicklung des cyber***Jack***® **e-com** unterstützt der cyber ***Jack***® **e-com plus** folgende Funktionen: Homebanking, elektronische Signatur, Bezahlen mit GeldKarte, EBICS, Secoder und eCard-API.

cyberJack® e-com plus

cyber*Jack*® secoder

Der cyber***Jack***® **secoder** ist das kleinste Mitglied der cyber***Jack***®-Familie. Dieser Chipkartenleser wurde speziell für das bequeme und sichere Onlinebanking mit der SECCOS-Bankenkarte entwickelt.

Der SECODER-Standard wurde von der deutschen Kreditwirtschaft spezifiziert. Ziel war es, einen einfachen und primär für das Onlinebanking optimierten Chipkartenleser zur definieren, damit Onlinetransaktionen durch eine Datenvisualisierung im Display des Chipkartenlesers noch besser abgesichert werden können.

Deshalb besitzt der cyber***Jack***® **secoder** unter anderem auch eine besondere Sicherheitsfunktion, die die sichere Anzeige der Onlinebanking-Transaktionsdaten unterstützt. So werden zum Beispiel Empfängerkontonummer und Betrag der Transaktionen im eigenen Display angezeigt. Angreifer, die versuchen die Empfängerkontonummer Ihrer Überweisung zu manipulieren, können Sie somit sofort entlarven. Denn die Anzeige des cyber***Jack***® **secoder** ist stets unabhängig von der Anzeige Ihres PC-Monitors und damit durch Trojaner oder Phisher nicht manipulierbar.

cyberJack® secoder

3 Chipkartenleser in Betrieb nehmen

3.1 Chipkartenleser auspacken und aufstellen

Auspacken

In der Verpackung sind enthalten[1)]:

- cyber***Jack***® Chipkartenleser
- Standfuß
- CD-ROM
- SIM-Adapterkarte (nicht bei cyber***Jack***® **secoder**)
- Kurzanleitung zur Geräteinstallation

1)
Sollten Sie das Gerät nicht direkt von REINER SCT beziehen, befinden sich unter Umständen noch weitere Komponenten in der Verpackung.

Aufstellen cyber*Jack*®

Bitte entnehmen Sie Gerät und Standfuß aus der Verpackung und schieben Sie den Standfuß in die Führung auf der Rückseite des Geräts komplett ein, so dass der Chipkartenleser einen sicheren Stand hat. Das Anschluss-Kabel können Sie in die am Standfuß angebrachte Kabelführung einlegen, so dass der Kabelabgang nach hinten erfolgt. Stellen Sie das Gerät so auf, dass Sie stets alle Bedienelemente im Blickfeld haben und bequem die Tastatur bedienen können.

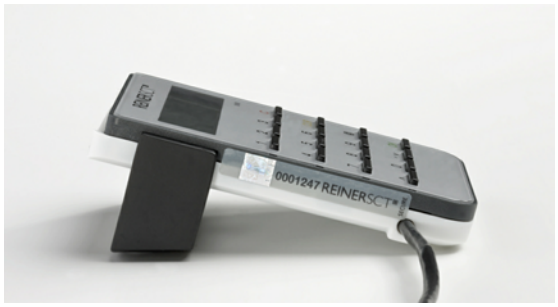
Sicherheitshinweis Gerätesiegel

Achten Sie darauf, dass das aufgebrachte Siegel unbeschädigt ist und der Abbildung auf dem Foto entspricht. Bei einer Beschädigung der Gerätesiegel besteht Manipulationsverdacht. Bitte wenden Sie sich in diesen Fall umgehend an Ihren Fachhändler und verwenden Sie das Gerät nicht.

Sicherheitsversiegelung
cyberJack pinpad/ e-com/ biometric

Sicherheitsversiegelung
cyberJack e-com plus

Sicherheitsversiegelung
cyberJack secoder, rechte Seite



Sicherheitsversiegelung
cyberJack secoder, linke Seite

3.2 Beschreibung der Bedienelemente

Aufnahme für Chipkarten

Die Chipkarten werden mit dem Chip voraus bis zum Anschlag in das Gerät eingesteckt. Der Chip zeigt dabei nach oben zur Tastaturseite.

Leuchtdioden (LEDs)

Grüne LED Anzeige des Betriebszustandes (nicht bei cyber***Jack***® **secoder**)
Gelbe LED Anzeige sicherer Betrieb, Anzeige Fehlerzustand

Display (nicht cyber*Jack*® pinpad)

Der cyber***Jack***® **e-com** und cyber***Jack***® **biometric** verfügen über ein Display mit zwei Zeilen á 16 Zeichen. Auf dem Display werden Steuertexte für die Eingabe der PIN ausgegeben. Bei GeldKarte-Anwendungen werden auf dem Display Zahlungsbetrag und -empfänger angezeigt.

Tastatur

0 - 9	Eingabe der PIN-Ziffern
OK	Bestätigung von Transaktionen, z.B. der eingegebenen PIN
CANCEL / C	Abbruch von Transaktionen
CLEAR / C	Funktion anwendungsspezifisch
@	Funktion anwendungsspezifisch
Pfeiltaste nach oben	Funktion anwendungsspezifisch
Pfeiltaste nach unten	Funktion anwendungsspezifisch

Biometrie-Modul (nur cyber*Jack*® biometric)

Der cyber***Jack***® **biometric** ist mit einem Fingerprint- Sensor ausgestattet, über den Fingerabdruck-Daten erfasst und ausgewertet werden können.

3.3 Maßnahmen zum sicheren Betrieb

Aufstellung des cyber*Jack*®

Stellen Sie die cyber***Jack***®-Chipkartenleser stets so auf, dass Sie die LEDs an der Gerätevorderseite im Blick haben. Die LEDs zeigen folgende Zustände an:

- Grüne LED leuchtet permanent (nicht bei cyber***Jack***® **secoder**)

Programm greift auf den Chipkartenleser zu

- Grüne LED blinkt (nicht bei cyber***Jack***® **secoder**)

Programm greift auf die Chipkarte zu

- Gelbe LED blinkt

Modus Sichere PIN-Eingabe/ Sichere Applikation ist aktiviert. Während des Modus Sichere PIN-Eingabe läßt der cyber***Jack***® keine Eingaben des PCs zu. Die Eingabe der PIN wird im Gerät zwischengespeichert. Während der PIN Eingabe zeigt der cyber***Jack***® den Text ‚Bitte Geheimzahl eingeben:' (bzw. ‚Neue Geheimzahl eingeben') gefolgt von einem ‚*' für jede eingegebene PIN-Ziffer an.

- Gelbe LED leuchtet permanent

Fehler (Falls trotz Ein- und Ausstecken des Geräts der Fehlerfall weiter besteht, kontaktieren Sie bitte den Support.)

Funktion Sichere PIN-Eingabe

Ihr cyber***Jack***®-Chipkartenleser verfügt über eine Funktion zur sicheren Eingabe von PINs. Die von Ihnen verwendete Applikation muss diese Funktion unterstützen! Die PIN wird über die interne Tastatur des Chipkartenlesers eingegeben. Bei der Funktion Sichere PIN-Eingabe darf die PIN nur eingegeben werden, wenn am Chipkartenleser die gelbe LED blinkt! Andernfalls werden Ihre Eingaben ggf. an den PC übertragen und können dort evtl. zu einem späteren Zeitpunkt ausgelesen werden. Die PIN-Eingabe wird mit [OK] bestätigt. Mit der [CANCEL-Taste] kann abgebrochen werden. Ausführliche Informationen zur Sicheren PIN-Eingabe finden Sie hier 17.

4 Installation der Hardware am PC

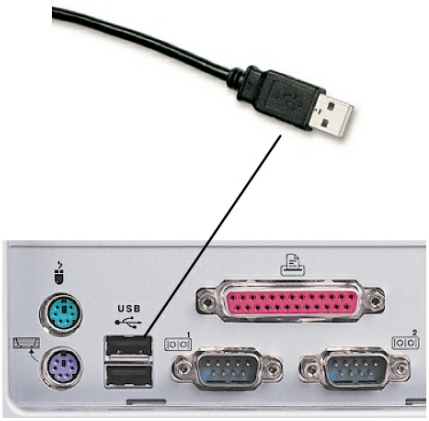
4.1 cyberJack USB

Der cyber***Jack***® mit USB-Anschluss darf erst nach erfolgter Installation des Treibers und erfolgtem Neustart an die USB-Schnittstelle des Rechners angeschlossen werden.
Der cyber***Jack***® USB wird an die USB-Schnittstelle Ihres Computers, bzw.an einen USB-Hub angeschlossen.

Bitte gehen Sie dazu folgendermaßen vor:

1. Installieren Sie zuerst die Treiber wie in Kapitel 5 beschrieben.
2. Stecken Sie anschließend den USB-Stecker des cyber***Jack***® **pinpad/e-com** USB in die entsprechende USB-Buchse Ihres PC ein. Sollten die vorhandenen USB-Schnittstellen Ihres Computers bereits belegt sein, benötigen Sie einen aktiven USB-Hub mit eigner Stromversorgung.
3. Ihr System zeigt nach wenigen Sekunden an, dass eine neue Systemkomponente gefunden wurde und der zugehörige Gerätetreiber installiert wird.

Die USB-Schnittstelle wird unter Windows von den Betriebssystemen Windows 2000/ XP/2003 Server/Vista sowie von Linux und MacOS unterstützt.



4.2 cyberJack TWIN seriell

Der cyber***Jack***® **pinpad/e-com** TWIN wird in die serielle PC-Schnittstelle (RS-232) eingeschleift. Zusätzlich wird die Stromversorgung über die Tastaturschnittstelle hergestellt.
Das Gerät funktioniert nur, wenn beide Schnittstellen angeschlossen sind!

Bitte gehen Sie dazu folgendermaßen vor:

1. Schließen Sie den seriellen Stecker des cyber***Jack***® **pinpad/e-com** (2) an die serielle Schnittstelle Ihres Rechners an.
2. Schließen Sie (für die Stromversorgung) den PS/2 Stecker (3) des cyber***Jack***® **pinpad/e-com** an die Tastaturbuchse Ihres Rechners an. Stecken Sie nun die Tastatur in die freie Buchse des cyber ***Jack***® **pinpad/e-com.** Bei Verwendung eines Notebooks schließen Sie den PS/2 Stecker an die Maus-/externe Tastaturbuchse an. Anschließend kann auch hier wiederum die Maus bzw. externe Tastatur angeschlossen werden.

Die serielle Schnittstelle wird unter Windows von den Betriebssystemen Windows 2000/ XP (nur 32 Bit)/2003 Server unterstützt.

Mit dem beigefügten Adapterkabel USB auf PS/2 kann der cyber***Jack***® auch unter XP 64 Bit/Vista 32/64 Bit/MacOS sowie Linux verwendet werden.

Adapterkabel USB - PS/2

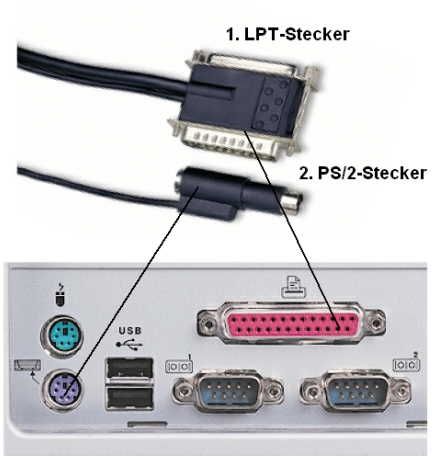
4.3 cyberJack LPT

Der cyber***Jack***® **pinpad/e-com** LPT wird in die parallele Druckerschnittstelle eingeschleift. Zusätzlich wird die Stromversorgung über die Tastaturschnittstelle hergestellt.
Das Gerät funktioniert nur, wenn beide Schnittstellen angeschlossen sind!

Bitte gehen Sie dazu folgendermaßen vor:

1. Schließen Sie den LPT-Stecker des cyber***Jack***® **pinpad/e-com** an die parallele Schnittstelle (Druckerschnittstelle) Ihres Rechners an. Sollte die Schnittstelle bereits durch einen Drucker, Scanner etc. belegt sein, so schließen Sie dieses Gerät nachfolgend an den LPT-Stecker des cyber ***Jack***® **pinpad/e-com** an. Bitte beachten Sie, dass der LPT Stecker der cyber***Jack***® **pinpad/e-com** immer direkt an der Schnittstelle des Computers stecken muss!
2. Schließen Sie (für die Stromversorgung) den PS/2 Stecker des cyberJack®pinpad/e-com an die Tastaturbuchse Ihres Rechners an. Stecken Sie nun die Tastatur in die freie Buchse des cyber***Jack*** ® **pinpad/e-com**. Bei Verwendung eines Notebooks schließen Sie den PS/2 Stecker an die Maus-/ externe Tastaturbuchse an. Anschließend kann auch hier wiederum die Maus bzw.externe Tastatur angeschlossen werden.

Die LPT-Schnittstelle wird unter Windows von den Betriebssystemen Windows 2000/XP (nur 32 Bit)/2003 Server unterstützt.



5 Installation der Softwarekomponente

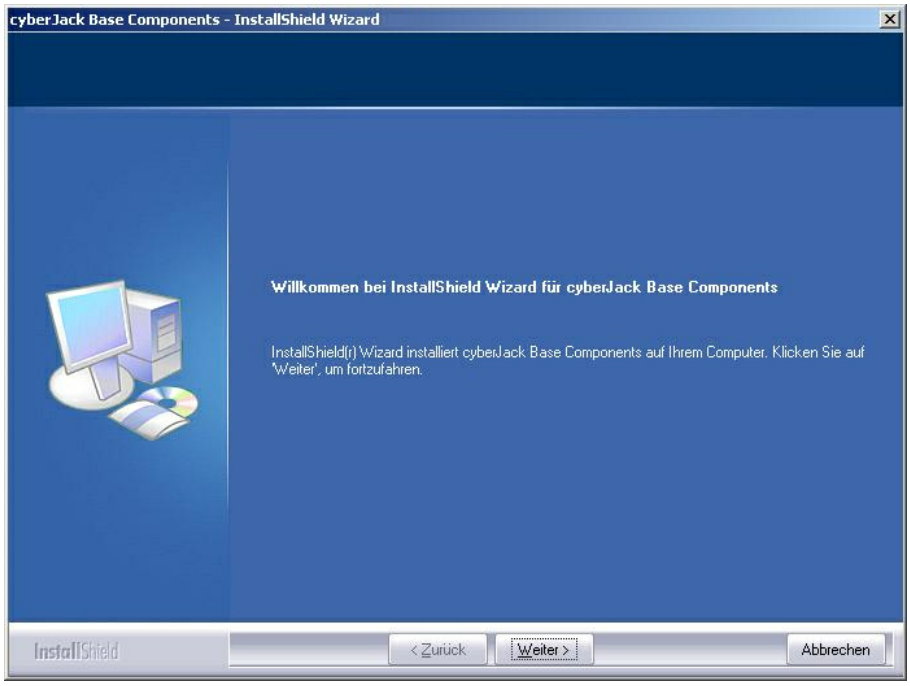
Legen Sie die cyber***Jack***® Treiber-CD in das CD-Laufwerk Ihres Computers ein. Mit dem daraufhin startenden Installation Manager können Sie verschiedene Softwarekomponenten für die cyber***Jack***® Chipkartenleserfamilie komfortabel und einfach installieren. Unterstützt Ihr System nicht die Autostart-Funktion, so starten Sie die Installation durch einen Doppelklick auf die Datei setup.exe, welche sich auf der CD befindet.

Durch die schnelle Entwicklung in der Computertechnologie kann es vorkommen, dass die Treiber auf der beiliegenden CD nicht immer auf dem aller neuesten Stand sind. Bitte nutzen Sie nach der Installation die Funktion „Prüfe auf neue Versionen“ (siehe 6.1 Gerätemanager) und führen Sie die ggf. angebotene Aktualisierung durch. So ist gewährleistet, dass Ihre Installation immer auf dem neuesten Stand ist.

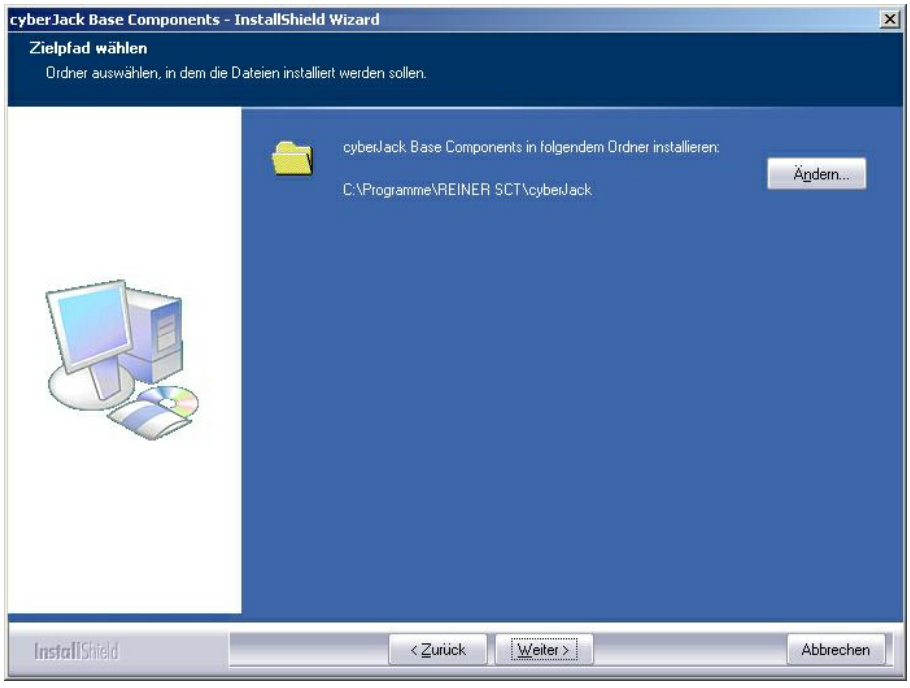
Die Installation cyber***Jack***® Base Components ist zum Betrieb der cyber***Jack***® Chipkartenleser unbedingt erforderlich. Hierin sind die Systemtreiber enthalten. Desweiteren wird der Gerätemanager mit den Funktionen Gerätetest, Treiberupdate und Online-Support installiert.

Betätigen Sie den Button [Installation starten], um mit der Installation der ausgewählten Komponenten zu beginnen. Werden über den Installation Manager mehrere Softwarekomponenten installiert, erfolgt ein notwendiger Neustart erst nach Installation der letzten Komponente.

Wollen Sie die cyber*Jack*® Base Components unter Windows 2000/XP/2003 Server/Vista installieren, müssen Sie über Administratorrechte verfügen. Beachten Sie weiterhin, dass alle Programme geschlossen werden müssen, bevor Sie mit der Installation beginnen.


cyberJack Base Components - InstallShield Wizard
Willkommen bei InstallShield Wizard für cyberJack Base Components
InstallShield(r) Wizard installiert cyberJack Base Components auf Ihrem Computer. Klicken Sie auf 'Weiter', um fortzufahren.
InstallShield
< Zurück
Weiter >
Abbrechen

Stimmen Sie im Fenster Lizenzvereinbarung den Lizenzvereinbarungen zu und klicken auf den Button [Weiter]. Wählen Sie im nächsten Schritt Ihre Anschlussart aus. Durch Anklicken des entsprechenden Kästchens wählen Sie den Treiber für Ihren Chipkartenleser aus. Klicken Sie auf [Weiter].



Klicken Sie auf [Weiter], wenn Sie das Programm indem angezeigten Ordner installieren wollen. Möchten Sie die Dateien in einem anderen Ordner installieren, klicken Sie auf [Ändern] und wählen Sie den gewünschten Pfad aus. Wählen Sie anschließend [Installieren] aus und die Installation der Treiber beginnt.

Nach Beendigung der Installation muss der PC nun neu gestartet werden, damit die installierten Treiber aktiviert werden. Im Windows Start-Menü wurde ein neuer Ordner REINER SCT cyberJack mit den Menüpunkten cyberJack Gerätemanager, Funktionstest, REINER SCT im Internet, Supportanfrage und ZKA Komponenten aktualisieren angelegt.

6 Die Funktionen Ihres Chipkartenlesers

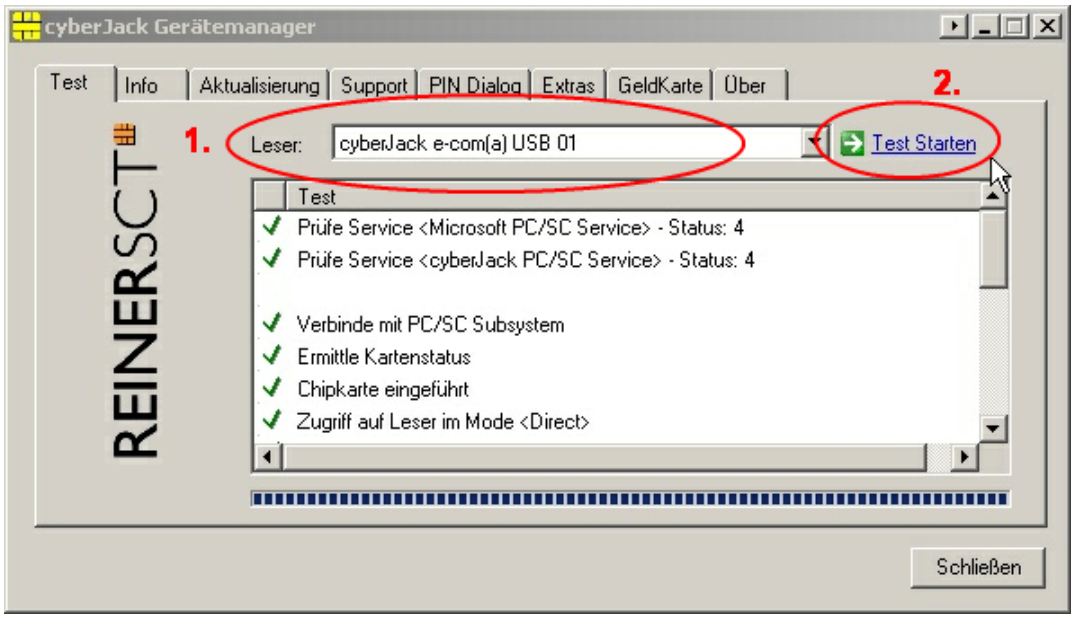
6.1 Gerätemanager

Der cyberJack Gerätemanager steht momentan nur für das Betriebssystem Windows zur Verfügung.

Starten Sie nach dem Neustart bitte das Programm cyberJack Gerätemanager, Funktionstest im Start-Menü unter Start > Programme > REINER SCT cyberJack. Beim Start des Gerätemanagers wird Ihnen ein Registrierungsdialog angezeigt. Wir empfehlen Ihnen, die Möglichkeit zur Registrierung zu nutzen, da Sie somit immer über neue Entwicklungen informiert werden, die Ihnen weiteren Nutzen zu Ihrem cyber***Jack***® bieten.

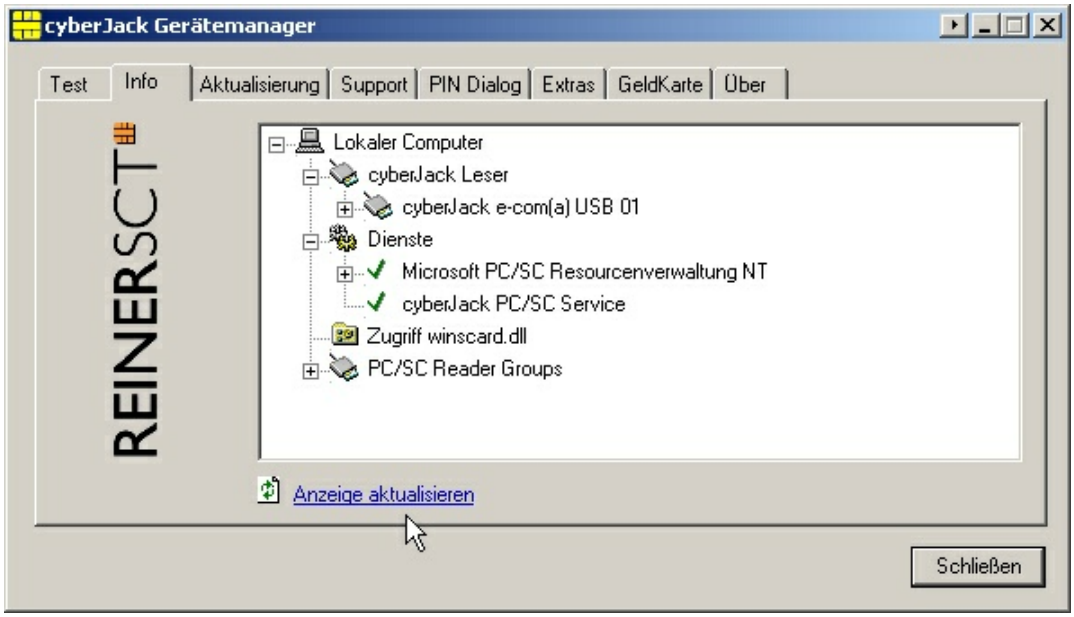
Registerkarte Test

Wenn Sie mehrere Chipkartenleser angeschlossen haben, können Sie unter (1) den entsprechenden Chipkartenleser auswählen. Nehmen Sie eine beliebige Chipkarte (GeldKarte, Telefonkarte, Versichertenkarte etc.) zur Hand, stecken Sie diese gemäß dem Symbol auf dem Gerät in den Schlitz des cyber***Jack***® bis zum Anschlag ein (die Karte verschwindet dabei etwa mit der halben Länge im Gerät) und betätigen Sie den Button [Test starten] (2). Es werden verschiedene Tests durchgeführt und dadurch überprüft, ob der cyber***Jack*** korrekt installiert wurde. Sollten beim Test Fehler auftreten, finden Sie Hilfe unter der Registerkarte Support. Hier können Sie sofort eine Verbindung zum Online-Testassistenten aufbauen und ein Fehlerprotokoll an unseren Support schicken.



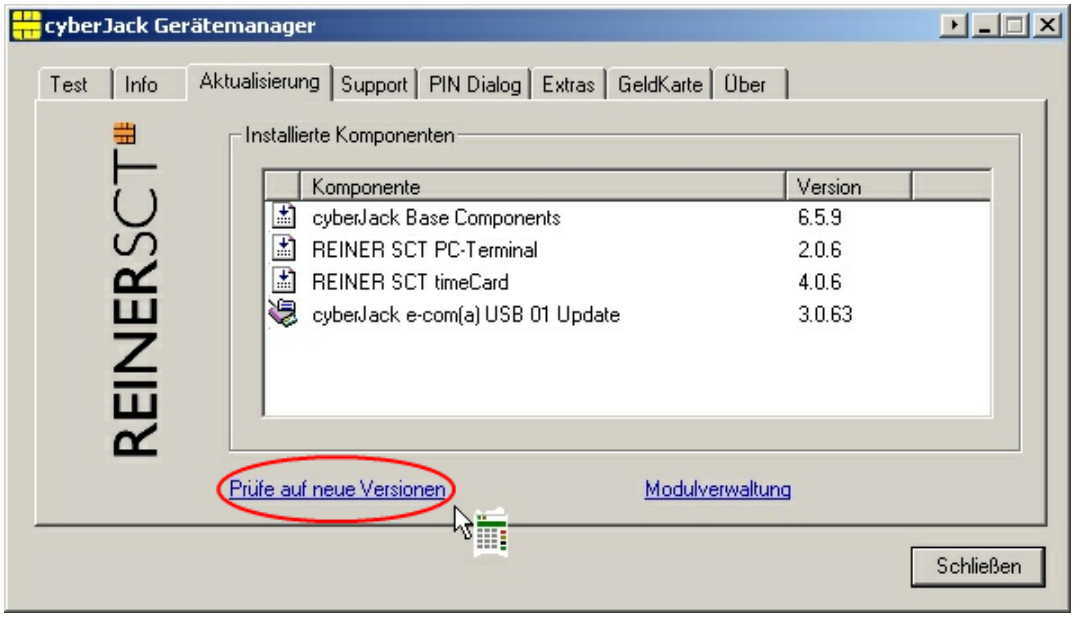
Registerkarte Info

Unter Info werden verschiedene Betriebs- und Konfigurationszustände des Chipkartenlesers sowie zugehöriger Komponenten angezeigt.



Registerkarte Aktualisierung

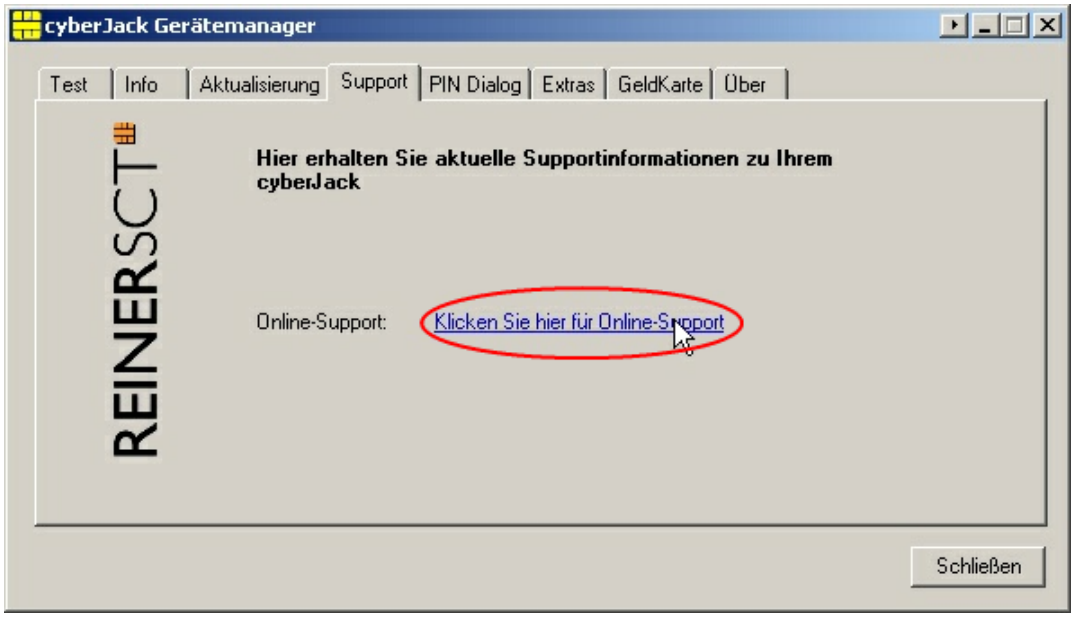
In Aktualisierung können Sie überprüfen, ob Sie noch über den aktuellen Treiberstand verfügen. Durch Betätigung des Links **Prüfe auf neue Versionen** wird Ihr Internet Browser gestartet und eine Verbindung zum REINER SCT Download Server hergestellt. Sollte Ihr Browser nicht standardmäßig mit einer DFÜ-Verbindung verknüpft sein, starten Sie diese bitte manuell, bevor Sie auf neue Versionen prüfen. Liegen neue Versionen vor, können Sie Ihr System direkt aktualisieren. Folgen Sie dazu der Menüführung.



Genauere Informationen zur Modulverwaltung erhalten Sie hier 21.

Registerkarte Support

Über Support haben Sie die Möglichkeit, direkt mit dem REINER SCT Support Kontakt aufzunehmen. Hierzu werden Ihre aktuellen cyber***Jack***® Installationsdaten zusammen mit einigen wichtigen Angaben zu Ihrer PC-Konfiguration ermittelt und per E-Mail an REINER SCT versandt. Einer unserer Supportmitarbeiter wird sich daraufhin mit Ihnen per E-Mail oder telefonisch in Verbindung setzen.

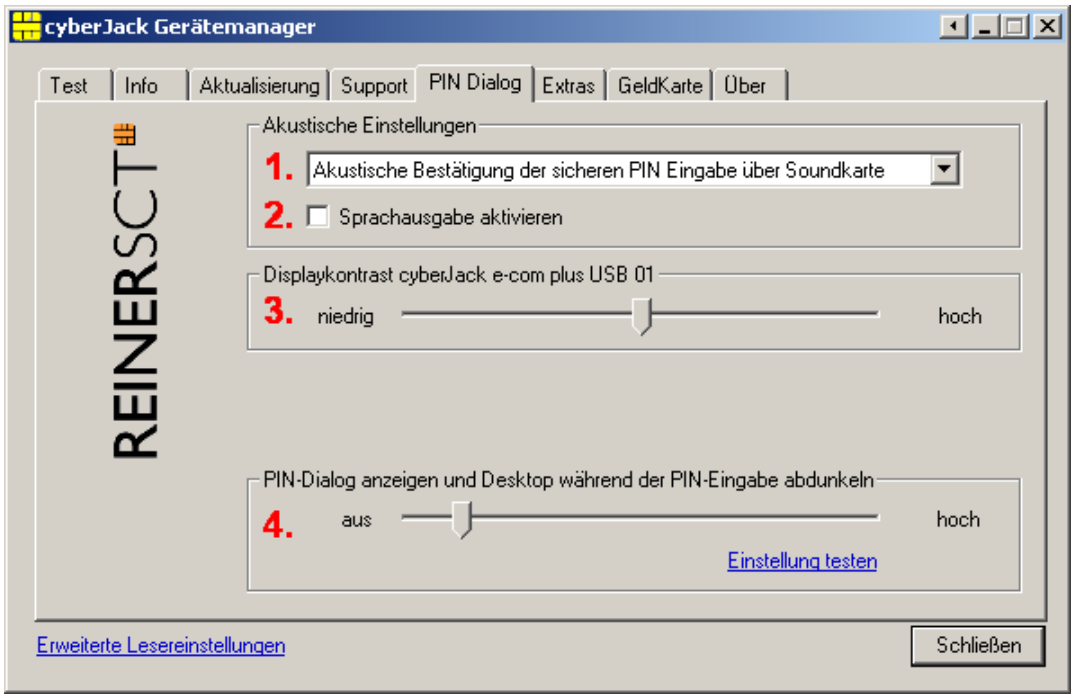


Registerkarte PIN Dialog

Im PIN Dialog sind aktivierbare Sonderfunktionen enthalten, mit denen bestimmte Sonderkonfigurationen eingestellt werden können. Diese werden zum Teil nur in sehr seltenen Fällen benötigt, weshalb Sie im Zweifelsfall die Auslieferungskonfiguration beibehalten sollten.

Akustische Einstellungen

(1) Hier können Sie auswählen, ob bei der PIN-Eingabe der Tastendruck ein Ton erzeugen soll.
(2) Setzen Sie hier den Haken und die Aufforderung der PIN ertönt akustisch mit einer freundlichen Stimme.
(3) Hier können Sie den Displaykontrast des Chipkartenlesers einstellen und somit die optimale Einstellung für das Ablesen des Chipkartenleserdisplays erzielen.
(4) Hier aktivieren Sie die PIN-Eingabe. Schieben Sie dazu den Schieberegler um mindestens eine Stufe nach rechts. Mit diesem Schieberegler wird auch der Grad der Abdunklung bei der PIN-Eingabe festgelegt. Über den **Button Einstellung testen** können Sie den Grad der Einstellung testen.



Die Sprachunterstützung und der PIN-Dialog wird bei der Ansteuerung der Chipkartenleser via PC/SC und CT-API unterstützt. Beide Funktionen sind aus

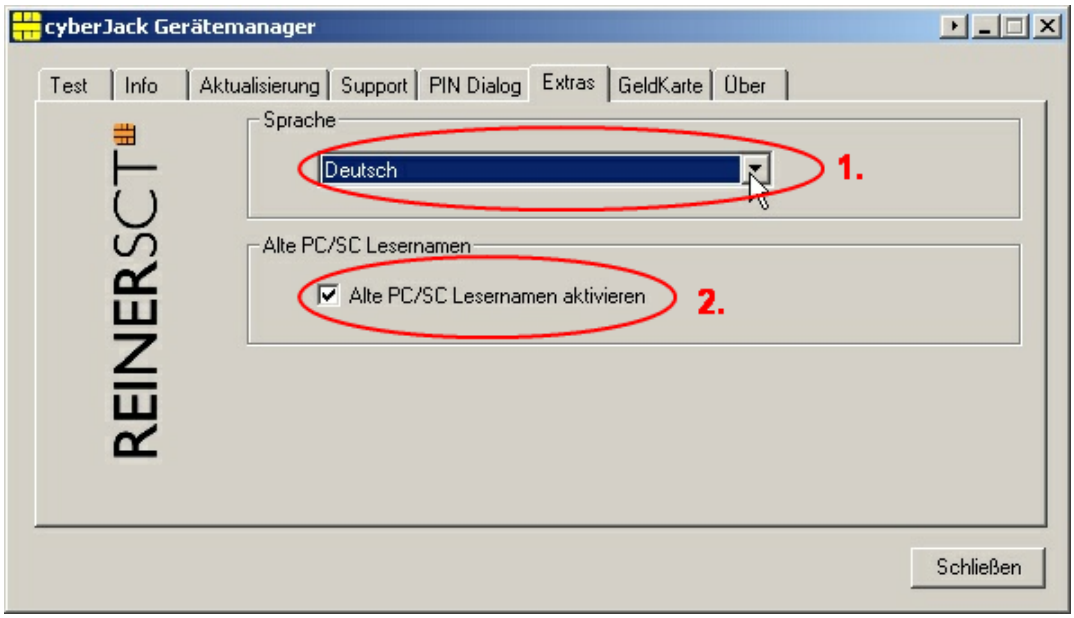
Kompatibilitätsgründen im Auslieferungszustand (Default) nicht aktiv.

Steht im Display des Chipkartenleser (außer cyber*Jack* pinpad) "Secoder", dann erfolgt keine akustische Bestätigung des Tastendrucks über die PC-Lautsprecher bzw. Soundkarte. Die Secoder-Spezifikation lässt dies aufgrund von Sicherheitsvorgaben nicht mehr zu.

Registerkarte Extras

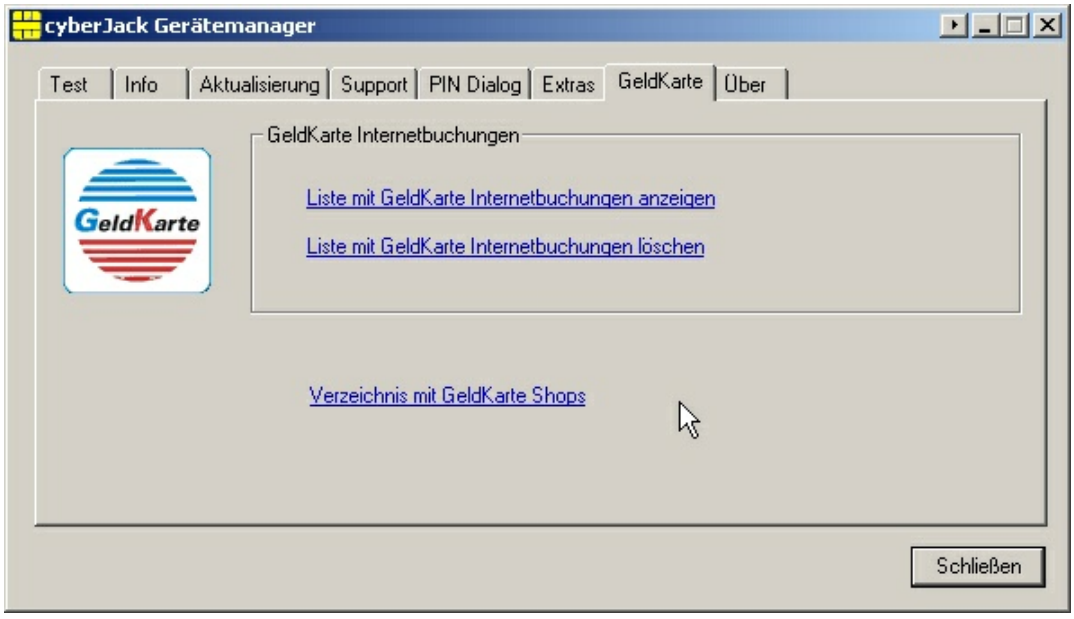
Hier können Sie die Sprache des Gerätemanagers (1) auswählen.

Bei einigen Signaturanwendungen kann es vorkommen, dass unsere Chipkartenleser nicht erkannt werden. Dann müssen die alten PS/SC Lesernamen aktiviert werden (2).



Registerkarte GeldKarte (nur cyber*Jack*® e-com)

Diese Registerkarte wird nur bei einem installierten cyber***Jack***® **e-com** angezeigt. GeldKarte-Transaktionen werden vom Chipkartenleser protokolliert und können mit den dargestellten Funktionen angezeigt bzw. gelöscht werden. REINER SCT pflegt ein Verzeichnis der Shops, bei denen mit der GeldKarte bezahlt werden kann. Dieses kann über den angegebenen Link direkt aufgerufen werden.



Registerkarte Über

Hier finden Sie die von Ihnen gemachten Registrierungsangaben, sowie einen direkten Link zur Homepage von REINER SCT, wo Sie sich über Produktneuheiten informieren können. Falls Sie sich noch nicht registriert haben, können Sie es hier jederzeit tun.

6.2 Die Funktion sichere PIN-Eingabe

Die Funktion Sichere PIN-Eingabe dient dazu, dass Ihre Geheimzahl in einer sicheren Umgebung bleibt. Verschiedene Hackerangriffe hatten bereits das Ausspähen der PIN zum Ziel. Die Angreifer machen sich hierbei die Tatsache zunutze, dass der PC eine unsichere Umgebung darstellt, bei der Tastatureingaben ohne Probleme aufgezeichnet und via Internet verschickt werden können. Die sichere Eingabe der PIN wird durch die PC-Anwendung gesteuert. Die allermeisten Programme in den Bereichen Homebanking und Elektronische Signatur unterstützen diese Funktion.

Sichere Eingabe der PIN

Wird die sichere PIN-Eingabe durch die Anwendung gestartet, kann die PIN innerhalb der vorgegebenen Zeit eingegeben werden.Die Zeit zwischen der Eingabe von zwei PIN-Ziffern liegt bei 5 Sekunden, wobei für jede PIN-Ziffer 5 Sekunden zur Verfügung stehen. Während beim cyber***Jack***® **e-com/e-com plus/secoder** der PIN-Dialog auf dem Display des Chipkartenlesers steht, werden für den cyber***Jack***® **pinpad** die folgenden Dialoge als virtuelles Display angezeigt. Die `*`-Zeichen stehen hierbei als Rückmeldung für einen Tastendruck. Die PIN-Ziffern selber verlassen den Chipkartenleser nicht und können aus diesem zu keinem Zeitpunkt ausgelesen werden.

cyberJack - Sichere PIN Eingabe
cyberJack - Sichere PIN Eingabe
Bitte geben Sie Ihre PIN an der Tastatur des Lesers ein und bestätigen Sie mit OK.
PIN: •••••_
Abbruch in 3 Sekunden

Sicheres Ändern der PIN

Um die PIN im sicheren Modus zu ändern, wird zuerst die aktuelle PIN eingegeben. Anschließend wird die neue PIN zweimal eingegeben. Jede Eingabe der PIN wird mit der [OK-Taste] bestätigt.

Das sichere Ändern der PIN wird nicht von allen Chipkarten unterstützt. Im Zweifel kontaktieren Sie bitte den Kartenemittenten (Bank,Trust-center etc.).

6.3 Integration des cyberJack-Chipkartenlesers in Anwendungen

Electronic Banking

Die Integration des Chipkartenlesers in die Homebanking-Anwendung geht in der Regel sehr einfach von statten. Viele Programme erkennen den cyber***Jack***® bereits automatisch. Manche Anwendungen verlangen nach einer Angabe der CT-API-DLL. Diese ist für alle Geräte der cyber***Jack***® Familie die ctrsct32.dll und steht im Windows Systemverzeichnis.

Elektronische Signatur

Softwarepakete zur Anwendung der elektronischen Signatur verwenden häufig die PC/SC-Schnittstelle. Die Treiber sind bereits im Betriebsystem enthalten.

GeldKarte

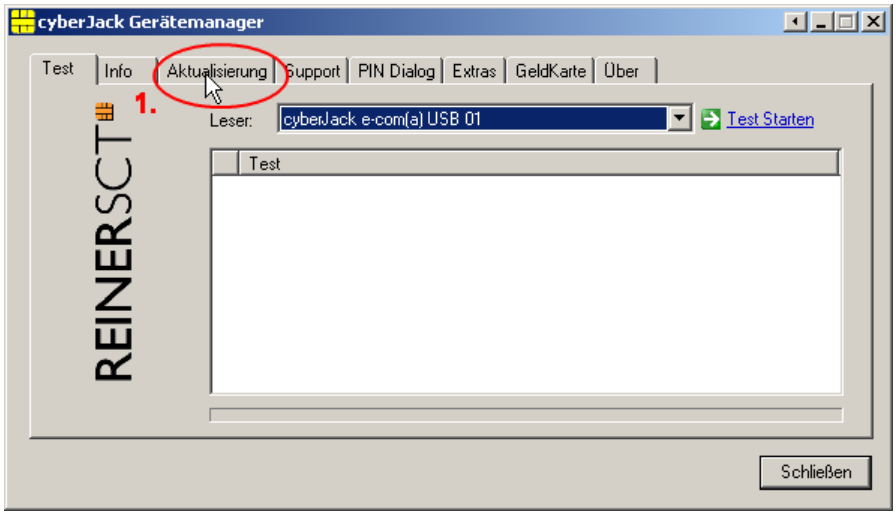
Hinweise zu Nutzungsmöglichkeiten der Geld-Karte im Internet erhalten Sie unter www.reiner-sct.com/geldkarte-shops.

6.4 TAN-Generierung nach HHD 1.3

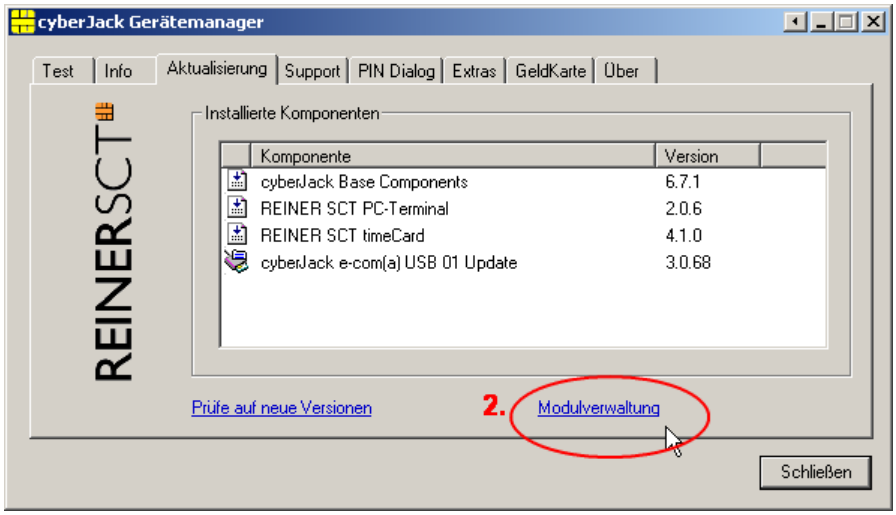
Die TAN-Generierung steht nur im cyber*Jack*® secoder, im cyber*Jack*® e-com (a) und im cyber*Jack*® e-com plus mit USB-Anschluss zur Verfügung. Im cyber*Jack*® pinpad , im cyber*Jack*® e-com (f) und im cyber*Jack*® biometric steht diese Funktion nicht zur Verfügung. Wie Sie einen cyber*Jack*® e-com (a) und einen cyber*Jack*® e-com (f) identifizieren können, erfahren Sie hier 37.

Um die TAN-Generierung nach HHD 1.3 nutzen zu können, müssen Sie das TAN-Modul in den Chipkartenleser laden. Gehen Sie dabei bitte wie folgt vor.

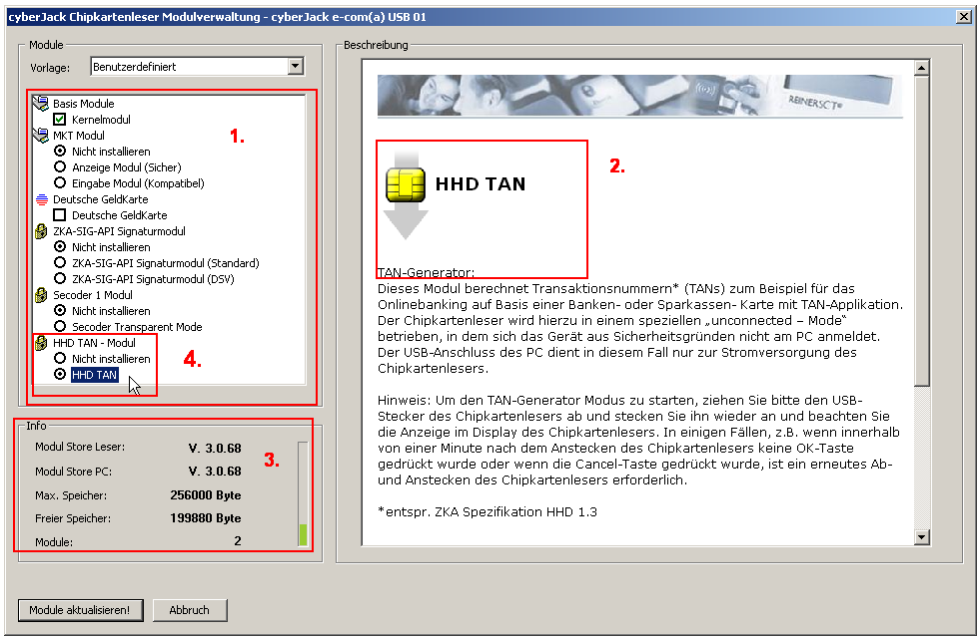
1. Schließen Sie den Chipkartenleser an Ihren PC an.
2. Starten Sie das Programm cyberJack Gerätemanager, Funktionstest im Start-Menü unter Start > Programme > REINER SCT cyberJack.
3. Wechseln Sie zum Reiter Aktualisierung (1).



4. Im Reiter Aktualisierung klicken Sie unten auf Modulverwaltung (2).



5. Es öffnet sich die Modulverwaltung. Auf der linken Seite (1) befinden sich die verfügbaren Module Ihres Chipkartenlesers. Auf der rechten Seite (2) finden Sie einige Erläuterungen zu den jeweiligen Modulen. Im Infofenster (3) erhalten Sie Angaben über die Speicherkapazitäten und die Versionsstände.


cyberJack Chipkartenleser Modulverwaltung - cyberJack e-com(a) USB 01
Module
Vorlage:
Benutzerdefiniert
Basis Module
Kernelmodul
MKT Modul
1.
Nicht installieren
Anzeige Modul (Sicher)
Eingabe Modul (Kompatibel)
Deutsche GeldKarte
Deutsche GeldKarte
ZKA-SIG-API Signaturmodul
Nicht installieren
ZKA-SIG-API Signaturmodul (Standard)
ZKA-SIG-API Signaturmodul (DSV)
Secoder 1 Modul
Nicht installieren
Secoder Transparent Mode
HHD TAN - Modul
Nicht installieren
HHD TAN
4.
Info
Modul Store Leser:
V. 3.0.68
Modul Store PC:
V. 3.0.68
3.
Max. Speicher:
256000 Byte
Freier Speicher:
199880 Byte
Module:
2
Beschreibung
HHD TAN
2.
TAN-Generator:
Dieses Modul berechnet Transaktionsnummern* (TANs) zum Beispiel für das Onlinebanking auf Basis einer Banken- oder Sparkassen- Karte mit TAN-Applikation. Der Chipkartenleser wird hierzu in einem speziellen „unconnected – Mode" betrieben, in dem sich das Gerät aus Sicherheitsgründen nicht am PC anmeldet. Der USB-Anschluss des PC dient in diesem Fall nur zur Stromversorgung des Chipkartenlesers.
Hinweis: Um den TAN-Generator Modus zu starten, ziehen Sie bitte den USB-Stecker des Chipkartenlesers ab und stecken Sie ihn wieder an und beachten Sie die Anzeige im Display des Chipkartenlesers. In einigen Fällen, z.B. wenn innerhalb von einer Minute nach dem Anstecken des Chipkartenlesers keine OK-Taste gedrückt wurde oder wenn die Cancel-Taste gedrückt wurde, ist ein erneutes Ab- und Anstecken des Chipkartenlesers erforderlich.
*entspr. ZKA Spezifikation HHD 1.3
Module aktualisieren!
Abbruch

6. Um das TAN-Modul zu laden, klicken Sie bei **HHD TAN-Modul** auf **HHD TAN** (4).
7. Anschließend klicken Sie auf den **Button Module aktualisieren**.
8. Beachten Sie die Anzeige Ihres Chipkartenlesers und bestätigen Sie die Aufforderungen des Chipkartenlesers mit der **OK-Taste**.
9. Nachdem alle Aktualisierungen abgeschlossen sind, können Sie alle Fenster des Gerätemanagers schließen.

10. Um jetzt den TAN-Generator Modus zu starten, ziehen Sie bitte den USB-Stecker des Chipkartenlesers ab und stecken Sie ihn wieder an. Beachten Sie die Anzeige im Display des Chipkartenlesers. Bestätigen Sie die Displayanzeige „TAN-Generator starten?“ mit der OK-Taste. In einigen Fällen, z.B. wenn innerhalb von einer Minute nach dem Anstecken des Chipkartenlesers keine OK-Taste gedrückt wurde oder wenn die Cancel-Taste gedrückt wurde, ist ein erneutes Ab- und Anstecken des Chipkartenlesers erforderlich.
11. Geben Sie nun den Start-Code ein, den Ihnen Ihre Online-Banking-Anwendung anzeigt. Folgen Sie dann den weiteren Anweisungen Ihrer Online-Banking-Anwendung. Mit der OK-Taste bestätigen Sie Ihre Eingaben.

Tastenfunktion bei der TAN-Generierung

OK-Taste:	Bestätigung der Eingabe
Cancel (C)-Taste:	Eingabe verwerfen
Clear (CLR)-Taste:	Letzte Eingabe löschen

Anzeige des ATC

Der ATC ist für eine Synchronisierung Ihrer Chipkarte mit Ihrer Bank oder Sparkasse notwendig. Ihr Online-Banking-System wird Sie ggf. auffordern diese Synchronisierung durchzuführen.
Die ATC-Anzeige erhalten Sie, wenn Sie bei angezeigter TAN die **@-Taste** betätigen

Aktivierung/ Deaktivierung der Funktion TAN-Generierung

Die Aktivierung bzw. Deaktivierung der Funktion TAN-Generierung kann nur durch Abziehen und Wiedereinstecken des USB-Steckers des Chipkartenlesegerätes erreicht werden.

TAN-Generator deaktivieren: Gerät an den PC anschließen und die Displayanzeige „TAN Generator starten?“ mit der **CANCEL-Taste** ablehnen.
TAN-Generator aktivieren: Gerät an den PC anschließen und die Displayanzeige „TAN Generator starten?“ mit der **OK-Taste** zustimmen.

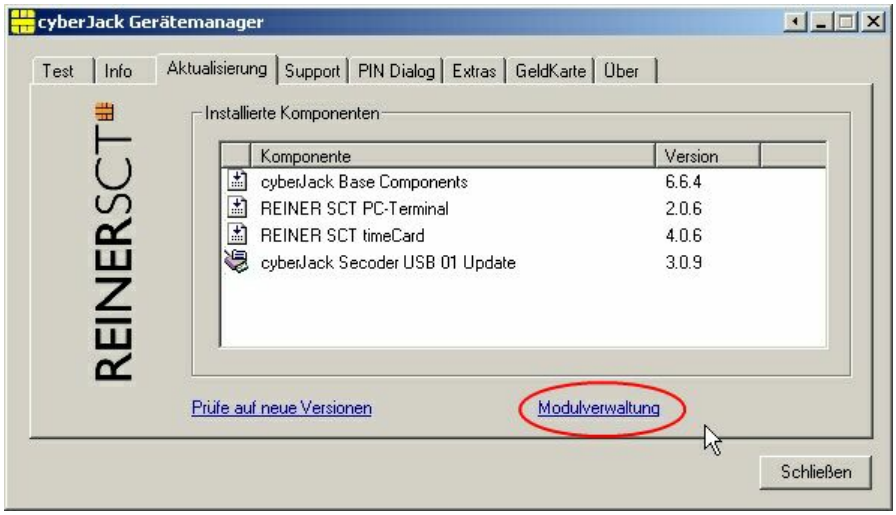
TAN-Funktion beim cyber*Jack*® secoder

In den cyber***Jack***® **secoder** kann immer nur ein Modul geladen und verwendet werden. Sollten Sie also den TAN-Generator deaktiviert haben, können Sie keine Secoder-Applikationen durchführen. Sie müssen erst wieder das Secoder Modul in den cyber***Jack***® **secoder** laden. Gehen Sie dabei bitte wie folgt vor.

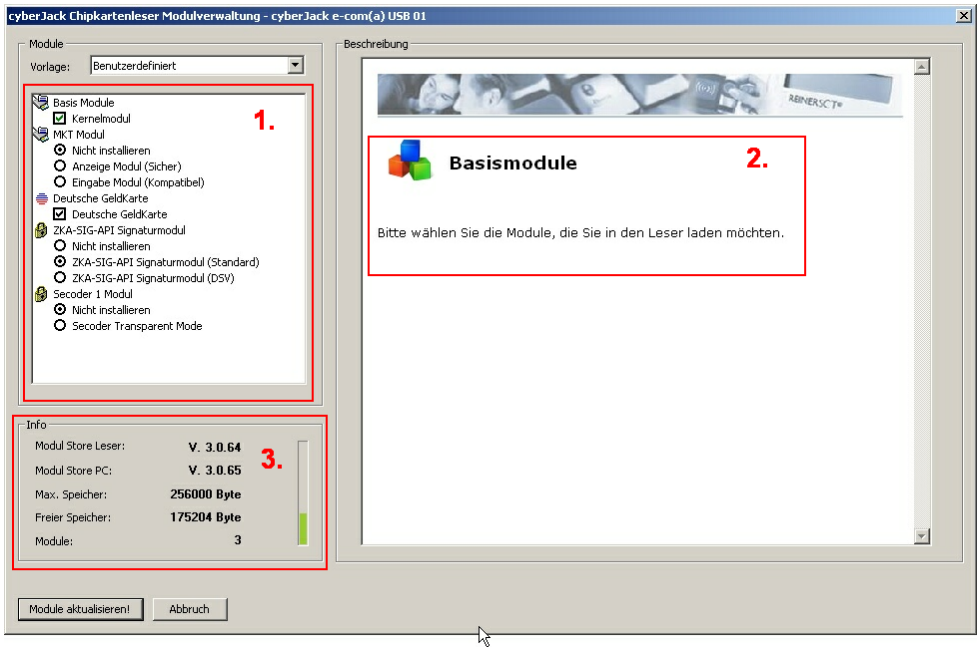
1. Schließen Sie den Chipkartenleser an Ihren PC an.
2. Starten Sie das Programm cyberJack Gerätemanager, Funktionstest im Start-Menü unter Start > Programme > REINER SCT cyberJack.
3. Wechseln Sie zum Reiter Aktualisierung.
4. Im Reiter Aktualisierung klicken Sie unten auf Modulverwaltung.
5. Es öffnet sich die Modulverwaltung. Wählen Sie auf der linken Seite bei **Secoder Modul** den **Secoder Transparent Mode** aus.
6. Betätigen Sie den **Button Module aktualisieren**.
7. Beachten Sie die Anzeige Ihres Chipkartenlesers und bestätigen Sie die Aufforderungen des Chipkartenlesers mit der **OK-Taste**.
8. Nachdem alle Aktualisierungen abgeschlossen sind, können Sie alle Fenster des Gerätemanagers schließen.
9. Im Display des cyber***Jack***® **secoder** steht nun Secoder 1. Die Secoder-Applikation ist geladen und kann verwendet werden.

7 Modulverwaltung

Mit der Modulverwaltung haben Sie die Möglichkeit verschiedene Module für unterschiedliche Anwendungen in Ihren Chipkartenleser zu laden.



Um in die Modulverwaltung zu gelangen, wechseln Sie im Gerätemanager in die Registerkarte **Aktualisierung**. Hier klicken Sie dann auf **Modulverwaltung**.



Auf der linken Seite (1) befinden sich die verfügbaren Module Ihres Chipkartenlesers. Auf der rechten Seite (2) finden Sie einige Erläuterungen zu den jeweiligen Modulen. Im Infofenster (3) erhalten Sie Angaben über die Speicherkapazitäten und die Versionsstände.

8 cyberJack biometric

Der cyber***Jack***® **biometric** basiert auf dem cyber***Jack***® **e-com**, der um ein Zusatzmodul zum Erfassen und Erkennen von Fingerabdrücken erweitert wurde. Alle für den cyber***Jack***® **e-com** beschriebenen Funktionen sind auch beim cyber***Jack***® **biometric** entsprechend vorhanden.

Funktionsprinzip

Das Biometriemodul des cyber***Jack***® **biometric** besteht aus einem Halbleiter-Sensor (CMOS-Technologie) und einer Auswerteeinheit. Der Sensor misst die Ladungsunterschiede zwischen den Fingerabdrucklinien und den Rillen und ermittelt daraus ein Graustufenbild des Fingerabdrucks. In einem zweiten Schritt wird dieses Bild ausgewertet, in dem die charakteristischen Merkmale des Fingers extrahiert und mit einem gespeicherten Referenzmuster verglichen werden. Das Referenzmuster wird beim erstmaligen Einlesen eines bestimmten Fingers (Enrollment) ermittelt. Im Gegensatz zu vielen biometrischen Systemen wird die sehr rechenintensive Bildauswertung nicht in den PC verlagert, wo Angriffe besonders leicht durchzuführen sind, sondern ist in den cyber***Jack***® **biometric** integriert, wodurch die Sicherheit maßgeblich gesteigert wird. Der cyber***Jack***® **biometric** arbeitet standardmäßig mit allen Applikationen zusammen, die die Funktion Sichere PIN-Eingabe unterstützen. Technische Informationen hierzu sind in Kapitel 9 enthalten.

Beim Enrollment werden Karte und Karten-PIN im Archiv des Biometriemoduls verschlüsselt gespeichert und einem Fingerabdruck zugeordnet. Ab jetzt reicht es aus, den Finger aufzulegen anstatt die PIN einzugeben.

Leistungsdaten

Es können maximal

- 10 Karten pro Finger
- 7 Verknüpfungen (4-Augenprinzip) pro Karte

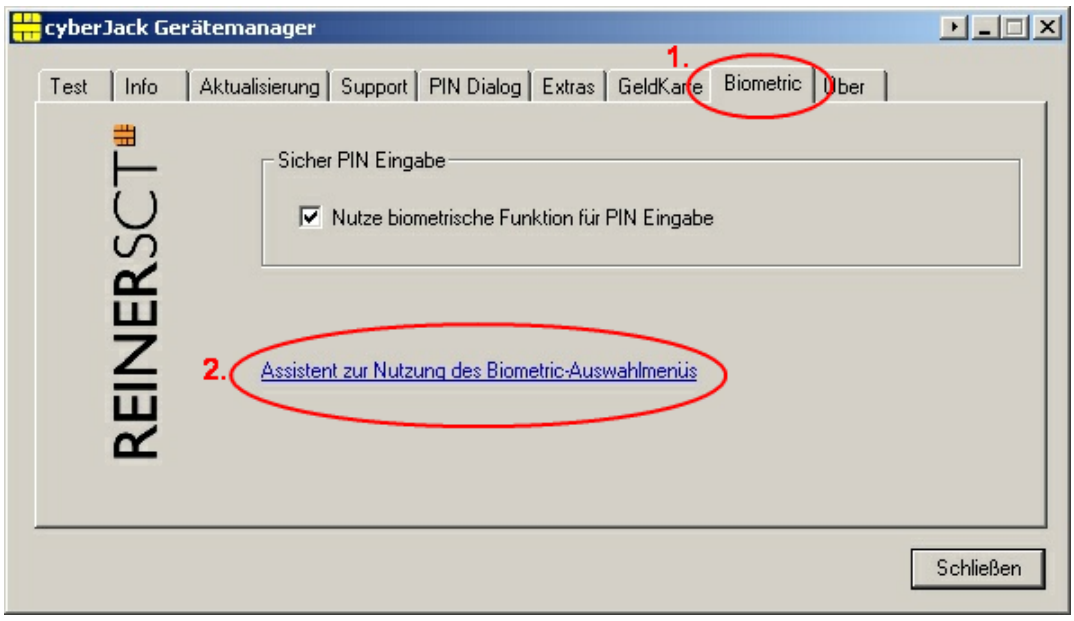
gespeichert werden. Weiterhin ist bei der Erstellung einer Verknüpfung die Eingabe der Karten-PIN notwendig. Es sind maximal 2 Fehlversuche dieser Karten-PIN pro Karte möglich.

Laut Signaturgesetz darf bei der qualifizierten elektronischen Signatur die PIN nicht gespeichert werden. Der cyber*Jack*® biometric ist deshalb für die qualifizierte elektronische Signatur nur ohne die Fingerabdruckfunktion geeignet. Geben Sie in diesem Fall bitte die PIN über die Tastatur des Chipkartenlesers ein.

Eine starke mechanische Beanspruchung der Hände kann dazu führen, dass ein Finger nicht erkannt wird. Umfangreiche Tests haben zwar ergeben, dass dies sehr selten vorkommt. Dennoch ist es parallel immer auch möglich, die PIN der Karte weiterhin über die Tastatur des Chipkartenlesers einzugeben.

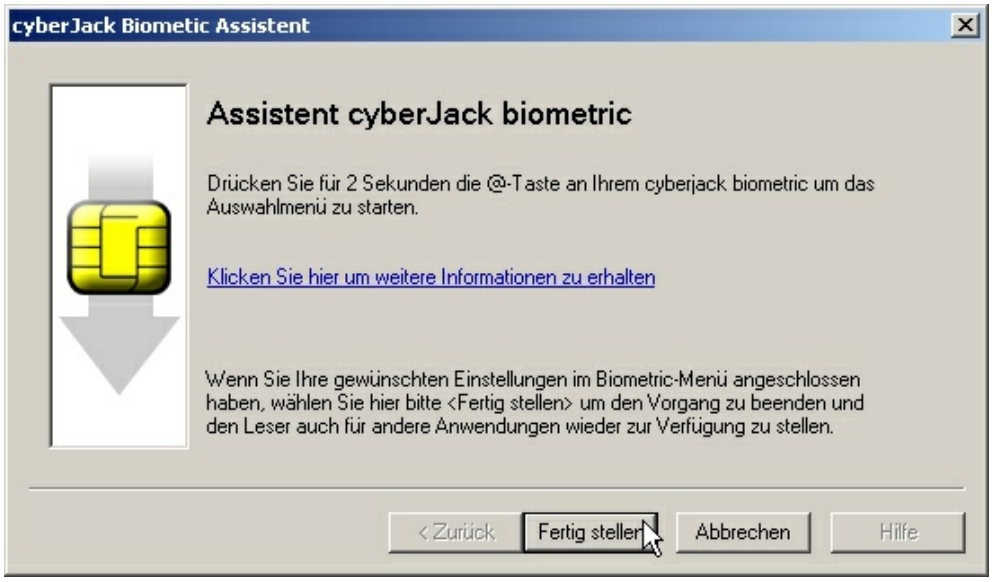
8.1 Menü

Um ins Funktionsmenü des cyber***Jack***® **biometric** zu gelangen, muss der Gerätemanager geöffnet sein. Im Gerätemanager wechseln Sie zum Register Biometric (1).



Wählen Sie hier Assistent zur Nutzung des Biometric-Auswahlmenüs (2) aus. Sie gelangen in folgenden Dialog.

Wählen Sie Ihren Chipkartenleser aus und drücken den Button **Weiter**. Das nun folgende Fenster muss während der gesamten Zeit der Einstellungen im Funktionsmenü des Biometric-Chipkartenlesers geöffnet bleiben.


cyberJack Biometic Assistent
Assistent cyberJack biometric
Drücken Sie für 2 Sekunden die @-Taste an Ihrem cyberjack biometric um das Auswahlmenü zu starten.
Klicken Sie hier um weitere Informationen zu erhalten
Wenn Sie Ihre gewünschten Einstellungen im Biometric-Menü angeschlossen haben, wählen Sie hier bitte <Fertig stellen> um den Vorgang zu beenden und den Leser auch für andere Anwendungen wieder zur Verfügung zu stellen.
< Zurück
Fertig stellen
Abbrechen
Hilfe

Erst wenn Sie alle Einstellungen vorgenommen haben, können Sie das Fenster schließen, in dem Sie den Button **Fertig stellen** drücken.

Das Funktionsmenü für die Biometriefunktionen wird durch 2 Sekunden langes Drücken der [@-Taste] aktiviert. Das Navigieren innerhalb des Menüs erfolgt über die Pfeiltasten oben/unten, die Auswahl eines Menüpunktes mit der [OK-Taste]. Das Drücken der [CANCEL-Taste] führt zum Verlassen des Menüs, die Betätigung der [CLEAR-Taste] löscht Eingaben bzw.springt in die nächst höhere Menüebene. Es stehen folgende Funktionen zur Verfügung:

- Erfassen
  - Enrollment
  - Quick-Enrollment
  - Weitere Karte
  - Verknüpfung
- Ändern
  - PIN
- Löschen
  - Karte
  - Verknüpfung
  - Finger
  - Komplettes Archiv
- Selbsttest

8.2 Erfassen

Enrollment/Quick-Enrollment

Das Enrollment bezeichnet das erstmalige Einlesen eines Fingerabdrucks. Aus dem Fingerbild wird ein Datensatz erzeugt, der für die zukünftige Erkennung als Referenz dient. Der Referenzdatensatz wird im Archiv des Fingerprint-Moduls des Chipkartenlesers verschlüsselt gespeichert.

Beim Enrollment wird der Bediener über das Gerätedisplay mehrere Male aufgefordert, den Finger aufzulegen und wieder abzuheben. Durch das Auflegen und Abheben des Fingers wird das Fingerbild in leicht veränderten Positionen erfasst, was die Qualität der späteren Erkennung verbessert.

Jeder Finger kann jedoch nur genau ein Mal im Archiv stehen. Der Versuch das Enrollment mit einem bereits gespeicherten Finger durchzuführen wird abgewiesen.

Bei der Funktion Quick-Enrollment wird der Vorgang durchgeführt, ohne dass zwischen den einzelnen Fingerscans zum Abheben des Fingers aufgefordert wird.

Vorgehen

1. Wählen Sie Erfassen > Enrollment/ Quickenrollment im Funktionsmenü aus.

2. Stecken Sie eine pingeschützte Chipkarte in den Chipkartenleser ein.
3. Geben Sie die PIN der Karte ein.
4. Legen Sie Ihren Finger auf und folgen den Anweisungen im Display. Das erfolgreiche Einscannen des Fingers wird mit **Enrollment erfolgreich** bestätigt.
5. Wollen Sie weitere Finger mit dieser Karte verknüpfen, wiederholen Sie bitte die Schritte 1-4.

Beim Enrollment ist es nicht möglich zu prüfen, ob die Karten-PIN korrekt ist. Wird zur Karte eine falsche PIN eingegeben, wird später bei Auflegen des Fingers auch die falsche PIN zur Karte geschickt, was im Wiederholungsfall zum Sperren der Chipkarte führen kann.

Weitere Karte

Mit dieser Funktion kann eine weitere Karte mit eigener PIN zu einem bestehenden Fingerabdruck hinzugefügt werden. Den bereits im Archiv hinterlegten Referenzdaten eines bereits enrollten Fingers wird eine weitere Karte inklusive PIN zugeordnet.

Vorgehen

1. Wählen Sie Erfassen > Weitere Karte im Funktionsmenü aus.
2. Stecken Sie eine weitere pingeschützte Chipkarte in den Chipkartenleser ein.
3. Geben Sie die PIN der Karte ein.
4. Legen Sie Ihren Finger auf und folgen den Anweisungen im Display. Das erfolgreiche Hinzufügen der Karte wird mit **Karte hinzufügen erfolgreich** bestätigt.
5. Wollen Sie weitere Karten einem bestehenden Fingerabdruck verknüpfen, wiederholen Sie bitte die Schritte 1-4.

Verknüpfung

Mit dieser Funktion wird das sogenannte 4-AugenPrinzip umgesetzt. Dies bedeutet, dass zur Freigabe der PIN zwei Finger benötigt werden. Diese können entweder zwei Personen (4-Augen-Prinzip) oder einer Person gehören. Hierzu müssen mit derselben Karte/PIN folgende Schritte durchgeführt werden:

Schritt 1	Enrollment Finger 1
Schritt 2	Enrollment Finger 2
Schritt 3	Erstellen der Verknüpfung

Vorgehen

1. Wählen Sie Erfassen > Verknüpfung im Funktionsmenü aus.
2. Stecken Sie eine pingeschützte Chipkarte in den Chipkartenleser ein.
3. Geben Sie die PIN der Karte ein.
4. Person 1 (P1:) legt den Finger auf. Finger wird gescannt.
5. Person 2 (P2:) legt den Finger auf. Finger wird gescannt. Das erfolgreiche Verknüpfen wird mit **Verknüpfung erstellt** bestätigt.
6. Wollen Sie weitere Verknüpfungen erstellen, wiederholen Sie bitte die Schritte 1-4.

Diese Funktion erlaubt es dem Inhaber von Karte/PIN zwei andere Personen zu autorisieren z.B. gemeinsam Banktransaktionen zu tätigen, ohne die PIN der Karte offen legen zu müssen. Diese Berechtigungen können, anders als wenn die PIN weitergeben würde, jederzeit vergeben und wieder gelöscht werden, zum Beispiel im Rahmen von Vertretungsregelungen.

8.3 Ändern

PIN

Mit dieser Funktion wird die zu einer Karte gespeicherte PIN geändert, wodurch allerdings nicht die PIN der Karte selbst geändert wird. Es ist deshalb unbedingt darauf zu achten, diese Funktion erst durchzuführen, wenn vorher auch die Karten-PIN entsprechend geändert wurde!

Die Karten-PIN ändern Sie mit Hilfe des Tools, welches Ihrer Chipkarte beiliegt.

8.4 Löschen

Karte

Mit dieser Funktion wird eine Karte aus dem Archiv gelöscht, während die Referenzdaten des Fingers erhalten bleiben. Dem Finger kann man dann wieder eine Karte unter Erfassen 25 zuweisen.

Verknüpfung

Diese Funktion löscht die Verknüpfung von zwei Fingern, so dass diese nicht mehr gemeinsam aufgelegt werden müssen, um die PIN an die Karte zu senden. Um eine Verknüpfung zu löschen, muss die zugehörige Karten-PIN bekannt sein und eingegeben werden.

Finger

Mit dieser Funktion werden die Referenzdaten eines Fingers aus dem Archiv gelöscht.

Komplettes Archiv

Mit dieser Funktion kann der Inhalt (Finger-Referenzdaten, Karten, PINs) des gesamten Archivs gelöscht werden.
Zum Löschen des Archivs ist die Eingabe folgender Archiv-PIN notwendig: **615243**.

8.5 Selbsttest

Mit der Funktion Selbsttest werden die Hardware-Komponenten des Biometriemoduls inkl. des Sensors überprüft. Ein erfolgreicher Test wird mit **Alle Komponenten betriebsbereit** bestätigt.

9 Support

Hilfe bei Störungen

Bei Störungen, die sich nicht durch eine erneute Inbetriebnahme (siehe Kapitel 2) Ihres cyber***Jack***® beheben lassen, kontaktieren Sie bitte unsere Serviceabteilung über die Funktion Support im Gerätemanager oder über unsere Website unter www.reiner-sct.com.

Service

Sie haben ein hochwertiges Produkt von REINER SCT erworben, das einer strengen Qualitätskontrolle unterliegt. Sollten trotzdem einmal Probleme auftreten oder haben Sie Fragen zur Bedienung des Gerätes, können Sie über den mit installierten Gerätemanager jederzeit eine Supportanfrage an unsere Serviceabteilung schicken.

Gewährleistung

REINER SCT leistet für Material und Herstellung des Chipkartenlesers eine Gewährleistung von 24 Monaten ab der Übergabe. Dem Käufer steht das Recht zur Nachbesserung zu. REINER SCT kann, statt nachzubessern, Ersatzgeräte liefern. Ausgetauschte Geräte gehen in das Eigentum von REINER SCT über.
Die Gewährleistung erlischt, wenn durch den Käufer oder nicht autorisierte Dritte in das Gerät eingegriffen wird. Schäden, die durch unsachgemäße Behandlung, Bedienung, Aufbewahrung, sowie durch höhere Gewalt oder sonstige äußere Einflüsse entstehen, fallen nicht unter die Garantie.

Schnittstelleninformationen für Entwickler

Um den cyber***Jack***® in Anwendungen zu integrieren gibt es zwei Schnittstellen: CT-API und PC/SC. Über diese greifen die Anwendungen auf die Chipkartenleser zu. Die CT-API-DLL hat die Bezeichnung ctrsct32.dll. Diese zu allen cyber***Jack***® Chipkartenlesern passende Datei befindet sich im Windows Systemverzeichnis. Weitere Informationen zu den Schnittstellenspezifikationen erhalten Sie bei Bedarf auf folgenden Websites:

CT-API www.teletrust.de
PC/SC www.pcscworkgroup.com

Entwickler, die die cyber***Jack***® Chipkartenleser in Ihre Anwendungen integrieren wollen, können sich mit Fragen jederzeit gerne an support@reiner-sct.com wenden.

10 Windows Terminal Server und CITRIX Administrator Guide

Hier erhalten Sie alle notwendigen Informationen zur Einrichtung und Nutzung von REINER SCT Chipkartenlesern unter Windows Terminal Servern (WTS) und CITRIX Presentation Servern (im Folgenden CITRIX genannt).

Dies ist ein Installationsleitfaden für Systemadministratoren. Im Folgenden werden Grundkenntnisse in der Administration von WTS bzw. CITRIX Servern und Clients vorausgesetzt.

1. Installationsvoraussetzungen

Es wird vorausgesetzt, dass ein WTS oder CITRIX Server bereits installiert und funktionsfähig ist. Alle Angaben in diesem Dokument beziehen sich auf Windows Terminal Server 2003 oder auf CITRIX Presentation Server 4.5. Wenn Sie andere Versionen einsetzen, so entnehmen Sie die entsprechenden Abweichungen bitte der Dokumentation der verwendeten Software.

1.1 Zugriff auf RDP Protokoll

Achtung: Windows 2000 Server unterstützt keine Smartcard Redirection.

Microsoft unterstützt zu diesem Zeitpunkt ausschließlich die Nutzung von an den Client angeschlossenen Chipkartenlesern aus einer Terminal Session. Der Zugriff auf Chipkartenleser aus einer Terminal Session auf einen lokal an den Server angeschlossenen Chipkartenleser ist somit nicht möglich.

Weitere Informationen zu diesem Thema gibt Microsoft Mitarbeiter Steve Patrick in seinem Blog:
http://blogs.msdn.com/spatdsg/archive/2006/10/16/smartcard-logon-over-terminal-services-rdp-redirection.aspx

Ein USB Extender „verlängert“ ein USB Kabel über ein Netzwerk. Aus Systemsicht ist ein über einen USB Extender angeschlossener Chipkartenleser mit einem lokal an den Server angeschlossenen Chipkartenleser gleichzusetzen

Der Zugriff aus einer Terminal Session auf einen Chipkartenleser, der über einen USB Extender mit den Server verbunden ist, ist somit nicht möglich.

1.2 Zugriff über ICA Protokoll

Die im vorherigen Kapitel genannten Einschränkungen gelten analog für das ICA Protokoll, nur ist es hier unter gewissen Systemversionen möglich die Smartcard Redirection zu deaktivieren.

Nähere Informationen erhalten Sie unter:
http://support.citrix.com/article/CTX107824

Wird die *Smartcard Redirection* deaktiviert, kann der Leser prinzipiell auch an den Server lokal angeschlossen werden. In virtuellen Umgebungen kann dann auch eine USB Redirection genutzt werden. Die weiteren Angaben in diesem Dokument treffen dann nicht mehr zu.

1.3 Zugriff über PC-Over-IP Protokoll (VM Ware View)

Das PCoIP Protokoll wurde zum Zugriff auf virtualisierte Desktops entwickelt. Das PCoIP Protokoll unterstützt die Smartcard Redirection. Der Chipkartenleser muss somit via Smartcard Redirection von Clients in den virtualisierten Desktop übernommen werden. Ein Mapping des Chipkartenlesers via USB Redirection ist nicht möglich. Die Installationsbedingungen sind analog zu denen des RDP/ICA Protokolls (WTS und CITRIX Server) ohne dass hierzu gesondert auf das PCoIP Protokoll hingewiesen wird. Auf Besonderheiten beim PCoIP Protokoll wird in den einzelnen Abschnitten gesondert hingewiesen.

2. Installationsplanung

Vor der Installation sollten folgende Punkte geklärt bzw. vorbereitet werden:

1. Welche Anwendung(en) sollen eingesetzt werden und welche Schnittstellen API (PC/SC oder CTAPI) werden von diesen Anwendungen benötigt?
2. Welche Chipkartenleser sollen verwendet werden?
3. Soll ein Thin- oder ein Fat-Client verwendet werden?

3. Serverinstallation

1. Installieren Sie die aktuelle Version der cyberJack Base Components auf Ihren Server. Die aktuelle Version können Sie sich unter http://www.reiner-sct.com herunterladen. Die Installation erfolgt i.d.R. mit einem Administratorenaccount innerhalb der Konsole des Servers.

Es werden folgende Funktionen installiert:
- Chipkartenleserunterstützung für lokal an den Server angeschlossene cyber***Jack*** Chipkartenleser
- cyberJack Gerätemanager/ Funktionstest für cyber***Jack*** Chipkartenleser innerhalb von WTS- und Citrix Sessions
- CTAPI Unterstützung für die WTS- und Citrix Clients

2. Deaktivieren Sie folgenden Service auf dem WTS / CITRIX Server:
- cyber***Jack*** PC/SC COM Service

3. Nur bei Zugriff über PCoIP
Die cyberJack Base Components können nicht automatisch erkennen das der Zugriff über das PCoIP Protokoll erfolgt. Dies muss über einen Registry-Eintrag manuell konfiguriert werden. Bitte fügen Sie in die Registry folgenden Wert ein:

Windows x32:
[HKEY_LOCAL_MACHINE\SOFTWARE\REINER SCT\cyberJack Base Components]
ForceWts=(DWORD) 1

Windows x64:
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\REINER SCT\cyberJack Base Components]
ForceWts=(DWORD) 1

Wird für eine Anwendung ausschließlich die PC/SC Schnittstelle benötigt, und werden keine Testtools benötigt, so kann auf die Installation der cyberJack Base Components auf dem Server verzichtet werden (nicht empfohlen).

4. Fat Client vs. Thin Client

Wird ein FAT Client (ein Windows-PC mit einer entsprechenden Terminalanwendung zum Zugriff auf den Terminal Server) eingesetzt, so können alle Chipkartenleser verwendet werden, die von den akt. cyberJack Base Components unterstützt werden. Soll ein Thin Client eingesetzt werden, so muss der Thin Client das gewünschte Chipkartenlesermodell nativ unterstützen oder es müssen die benötigten Treiber - sofern möglich - nachträglich installiert werden.
(Siehe Kapitel 4.2 Thin Clients)

4.1 Fat Clients

Die Verwendung von Fat (Windows) Clients ist sowohl für WTS, als auch für CITRIX Umge-bungen Out-of-the-box möglich.
Sie können innerhalb einer WST- oder CITRIX Session alle REINER SCT Chipkartenlesermodelle verwenden. Eine gleichzeitige Nutzung des Chipkartenlesers durch Anwendungen, die innerhalb der WTS- oder CITRIX Session und Anwendungen, die lokal auf den Client laufen, ist problemlos möglich.

Installation:

1. Installieren Sie die aktuelle Version der cyberJack Base Components auf Ihren PC. Die aktuelle Version können Sie sich unter http://www.reiner-sct.com herunterladen.

2. Führen Sie einen lokalen Funktionstest mit dem cyberJack Gerätemanager (Start -> Programme -> REINER SCT cyberJack -> cyberJack Gerätemanager / Funktionstest) durch.

3. Überprüfen Sie, ob die Verwendung (Redirection) von lokalen Smartcard Ressourcen innerhalb des Terminal Clients aktiviert ist. Informationen hierzu entnehmen Sie bitte dem CITRIX Produkthandbuch.

4. Überprüfen Sie ob Verwendung (Redirection) der seriellen Schnittstellen innerhalb des Terminal Clients aktiviert ist (nur notwendig ab BC 6.7.1). Die serielle Schnittstelle wird benötigt, um Statusinformationen zwischen WTS-Client und Server zu übertragen.

   Die Info Extension steht nur unter Windows basierenden Clients zur Verfügung. Ist diese aktiv, so stehen im cyberJack Gerätemanager die selben Informationen zur Verfügung, wie bei einem lokal aufgerufenen cyberJack Gerätemanager. Steht die Info Extension nicht zur Verfügung, so werden einige Statusinformationen nicht angezeigt. Die Funktion des Chipkartenlesers wird hierdurch aber nicht beeinflusst.

Hinweis:
Bis zur Version < V 6.7.1 der cyberJack Base Components steht die Info Extension nur unter WTS mit einem RDP Client < V 6.0, nicht aber unter CITRIX zur Verfügung.

Zur Nutzung der ZkaSig Schnittstelle unter WTS / CITRIX wird die Info Extension benötigt.

Per Default wird zur Übertragung der Daten der Info Extension der virtuelle COM Port 10 verwendet. Sollte dieser von einer anderen Anwendung belegt sein, so können Sie diesen über die folgende Registry Einträge ändern:

WTS/CITRIX Client:

[HKEY_LOCAL_MACHINE\SOFTWARE\REINER SCT\cyberJack Base Components]
WtsComPort=(DWORD) <Nummer des COM Ports>

WTS/CITRIX Server Session:

[HKEY_CURRENT_USER\SOFTWARE\REINER SCT\cyberJack Base Components]
WtsComPort=(DWORD) <Nummer des COM Ports>

Die Installation ist nun soweit abgeschlossen. Fahren Sie nun bitte mit 5. Testen der Installation fort.

4.2 Thin clients

Die Verwendung von Thin Clients ist nur möglich, wenn auf dem Client eine Unterstützung für das entsprechende cyber***Jack*** Modell integriert ist, d.h. die benötigten Treiber installiert sind.

Eine Reihe von Herstellern bietet Thin Clients mit vorinstallierter Treiberunterstützung für cyber***Jack*** Chipkartenleser an.

Prüfen Sie bitte in der Dokumentation Ihres Gerätes, ob der gewünschte cyber***Jack*** Chipkartenleser unterstützt wird. Oftmals bieten die Hersteller der Thin Clients aktualisierte Images an, welche das gewünschte Gerät unterstützen.

Unterstützt Ihr Thin Client den gewünschten cyber***Jack*** Chipkartenleser 'out-Of-the-box', so schließen Sie diesen bitte an (Dokumentation des Thin clients beachten) und fahren Sie mit 5. Testen der

Installation fort.

Sollte der Hersteller des Thin clients keine Unterstützung für den gewünschten cyber***Jack*** Chipkartenleser anbieten, so prüfen Sie bitte ob es möglich ist, Treiber auf das Image des Thin Clients nach zu installieren. Treiber stehen für alle gängigen Thin-Client Betriebssysteme (LINUX, XP embedded und Windows CE) zur Verfügung. Die benötigten Treiber erhalten Sie über unsere Homepage unter http://www.reiner-sct.com oder wenden Sie sich an unseren Support (support@reiner-sct.com).

Die Vorgehensweise zur Installation von Treibern auf Thin-Client Geräten ist sehr unterschiedlich, die notwendigen Informationen entnehmen Sie bitte der Dokumentation des Geräte-Herstellers.

5. Testen der Installation

1. Öffnen Sie nun den RDP- oder ICA Client und melden Sie sich an.

   Starten Sie nun den cyber***Jack*** Gerätemanager und Funktionstest innerhalb der Terminal Server Session.

   Sie werden bemerken, dass nun gegenüber den Aufruf auf dem lokalen PC einen weiteren Reiter mit der Bezeichnung <WTS> zur Verfügung steht. Auf dieser Seite erhalten Sie Informationen zur aktuellen Terminal Server Session.

   Die Werte für Protokoll und Typ geben Informationen über den Terminal Server Typ und das verwendete Terminal Server Protokoll.

   Die Info Extension steht nur unter WTS und einem FAT Windows Client zur Verfügung. Ist diese aktiv, so stehen im cyber***Jack*** Gerätemanager dieselben Informationen zur Verfügung wie bei einem lokal aufgerufenen cyber***Jack*** Gerätemanager. Steht die Info Extension nicht zur Verfügung, so stehen einige Informationen nicht zur Verfügung.

   Der Wert für PC/SC Status gibt an, ob eine Verbindung mit den PC/SC Subsystem des Clients möglich ist oder welcher Fehler gemeldet wird. Anhang B dieses Dokuments enthält eine Auswahl mit typischen Fehlern.

2. Wechseln Sie auf den Reiter <Test> und führen Sie einen Funktionstest durch.
   Werden alle Tests korrekt durchlaufen, so ist der Chipkartenleser nun einsatzbereit.

6. Konfigurationsdatei hbcikrnl.ini

Während der Installation der cyberJack Base Components wird eine Konfigurationsdatei hbcikrnl.ini angelegt, in der alle installierten CTAPI Chipkartenleser eingetragen werden.

Die hbcikrnl.ini wird entsprechend dem Standard im Verzeichnis c:\windows erstellt. Je nach Konfiguration des Servers findet allerdings eine Virtualisierung des Verzeichnisses statt, so dass die Datei im virtualisierten Verzeichnis C:\Dokumente und Einstellungen\<Benutzerkonto>\WINDOWS angelegt wird.

Wenn Ihre Anwendung diese Datei verwendet, so ist es nötig die Datei in jedes virtualisierte Windows Verzeichnis zu kopieren.

http://etutorials.org/Microsoft+Products/microsoft+windows+server+2003+terminal+services/Chapter+6+Registry/Compatibility+Flags/

7. Hinweis zur Nutzung von SFIRM

SFIRM wird von den cyberJack Base Components nativ unterstützt. Die Installation von STAN (-> http://www.sfirm.de/index.php?id=546=) ist somit bei der Nutzung mit cyber***Jack*** Chipkartenlesern

nicht erforderlich.

8. Hinweis zur Nutzung unter LINUX mit rdesktop und CTAPI:

Wenn in einer RDP oder ICA Session via rdesktop (oder einem anderen RDP/ICA Client) via CTAPI auf den Chipkartenleser zugreifen möchten,
so beachten Sie bitte folgendes:

1. Auf dem Windows Server muss mindestens die Version 6.7.4 der cyberJack Base Components installiert sein.
2. Auf dem LINUX Terminal muss mindestens die Version 3.3.2 der Linux Treiber installiert sein.
3. Das PC/SC device renaming feature (z.B. rdesktop -r scard:"CyberJack pp_a 00 00"=....) darf nicht verwendet werden.

Weiterführende Informationen / Links

1.) Microsoft: Steve Spate Blog Smartcard logon over Terminal Services (RDP redirection)
http://blogs.msdn.com/spatdsg/archive/2006/10/16/smartcard-logon-over-terminal-services-rdp-redirection.aspx

2.) Overview of the Citrix Support for Smart Card Software
http://support.citrix.com/article/ctx105027/

3.) Microsoft: Smartcard - So wird es gemacht...
http://technet2.microsoft.com/windowsserver/de/library/70e8db04-d7dc-406b-9759-80ddc87e35ef1031.mspx?mfr=true

4.) Microsoft: The Smart Card Deployment Cookbook
http://www.microsoft.com/technet/security/guidance/identitymanagement/smrtcdcb/default.mspx

5.) Microsoft: Planning Your Public Key Infrastructure
http://www.microsoft.com/technet/prodtechnol/windows2000serv/reskit/deploy/dgch_pki_odbg.mspx?mfr=true

6.) CITRIX: How To Disable SmartCard Authentication for Windows Logon
http://support.citrix.com/article/CTX116151

7.) Microsoft: Smart Cards Check Box Does Not Appear on the Local Resources Tab in the Remote Desktop Connection Dialog Box
http://support.microsoft.com/kb/820525/en-us

Auswahl Windows Fehlercodes

Status	Beschreibung
OK	Es wurde (mind.) ein Chipkartenleser gefunden
0x8010001D	Das PC/SC Subsystem ist nicht aktiv. 1. Möglicher Grund: Lokale Smartcard Ressourcen nicht aktiviert 2. Eine lokale Richtlinie verbietet die Smartcard Redirection **Windows Server 2008:** ->Computerkonfiguration -> Richtlinien -> Administrative Vorlagen -> Windows Komponenten -> Remotedesktopdienste -> Remotedesktopsitzungs-Host ->Geräte- und Ressourcenumleitung -> "Keine Geräteumleitung für Smartcards zulassen".

	Windows Server 2008: ->Computerkonfiguration -> Richtlinien -> Administrative Vorlagen -> Windows Komponenten -> Terminalserver -> Geräte- und Ressourcenverwaltung -> "Keine Geräteumleitung für Smartcards zu-lassen".
0x8010002E	Es wurde kein Chipkartenleser gefunden. Möglicher Grund: Der Chipkartenleser wird am Client nicht erkannt.
0x0000006D	Der Windows Fehler ERROR_BROKEN_PIPE wird angezeigt wenn das Betriebssystem keine Smartcard Aktionen unterstützt. (->*http://msdn.microsoft.com/enus/library/aa374738(VS.85).aspx*)

ThinClients mit integrierter cyber*Jack* Chipkartenleser Unterstützung

Die folgenden Tabellen geben einen Überblick über die Unterstützung der cyber***Jack*** Chipkartenleser einzelner Thin-Client Modelle. Ist das benötigte Thin-Client Modell nicht aufgeführt, so konsultieren Sie bitte die Dokumentation des Thin-Clients Geräts oder kontaktieren Sie den Hersteller des Thin-Clients.

Hersteller Fujitsu Technology Solutions							
Modell	pinpad 2.0	pinpad(a) 3.0	e-com 2.0	e-com(a) 3.0	secoder	e-com +	e-com (f)
Futro C100 (Board D1544)	-	+	-	+	+	+	+
Futro C100 (Board D1544)	-	+	-	+	+	+	+
Futro C200 (Board D1944)	-	+	-	+	+	+	+
Futro C250 (Board D1784)	-	+	-	+	+	+	+
Futro S100 (Board D2456)	-	+	-	+	+	+	+
Futro S450 (Board D2703)	-	+	-	+	+	+	+
Futro S500 (Board D2703)	-	+	-	+	+	+	+
Futro S550 (Board D2703)	-	+	-	+	+	+	+
Esprimo C5720 (Board D2764)	-	+	-	+	+	+	+
Esprimo C5730 (Board D2804)	-	+	-	+	+	+	+
Esprimo C5910 (Board D2364-A3)	-	+	-	+	+	+	+
Esprimo E5720 (Board D2764)	-	+	-	+	+	+	+
Esprimo E5730 (Board D2824)	-	+	-	+	+	+	+
Weitere Modelle des Herstellers mit eLux ab V 2.2	-	+	-	+	+	+	+

Weitere Modelle des Herstellers mit XP embedded	+	+	+	+	+	+	+

Hinweis:

1. Es wird eLux RL (Linux-Kernel 2.6) benötigt

2. Zur Unterstützung der Reiner SCT-Chipkartenleser wurde aktuell ein device handler in eLux RL integriert. Die eLux RL-Version mit dieser Funktionalität wird ab Oktober 2009 im myelux.com-Portal zur Verfügung gestellt.
   Registrierte Benutzer werden gesondert informiert.

3. Unter eLux NG (Linux-Kernel 2.4)wird ausschließlich der pinpad (a) 3.0 (PID:0x300) unterstützt. Ein Update von eLux NG auf eLux RL ist ab Scout Version 11 möglich.

4. Sollten Sie über ein nicht aufgeführtes Modell des Herstellers verfügen, so konsultieren Sie bitte die technische Dokumentation des Thin-Clients ob der gewünschte Chipkartenleser unterstützt wird.

Hersteller Hewlett Packard							
Modell	pinpad 2.0	pinpad(a) 3.0	e-com 2.0	e-com(a) 3.0	secoder	e-com +	e-com (f)
T5545	-	+	-	+	+	+	+
T5735	-	+	-	+	+	+	+
st5738	-	+	-	+	+	+	+
st5548	-	+	-	+	+	+	+
Weitere Modelle des Herstellers mit eLux ab V 2.2	-	+	-	+	+	+	+
Weitere Modelle des Herstellers mit XP embedded	+	+	+	+	+	+	+

Hinweis:

1. Es wird eLux RL (Linux-Kernel 2.6) benötigt.

2. Zur Unterstützung der Reiner SCT-Chipkartenleser wurde aktuell ein device handler in eLux RL integriert. Die eLux RL-Version mit dieser Funktionalität wird ab Oktober 2009 im myelux.com-Portal zur Verfügung gestellt.
   Registrierte Benutzer werden gesondert informiert.

3. Unter eLux NG (Linux-Kernel 2.4)wird ausschließlich der pinpad (a) 3.0 (PID:0x300) unterstützt. Ein Update von eLux NG auf eLux RL ist ab Scout Version 11 möglich.

4. Sollten Sie über ein nicht aufgeführtes Modell des Herstellers verfügen, so konsultieren Sie bitte die technische Dokumentation des Thin-Clients ob der gewünschte Chipkartenleser unterstützt wird.

Hersteller Igel							
Modell	pinpad 2.0	pinpad(a) 3.0	e-com 2.0	e-com(a) 3.0	secoder	e-com +	e-com (f)
Universal Desktop Converter	+	+	+	+	+	+	+
IGEL one	+	+	+	+	+	+	+
Universal Desktop Series	+	+	+	+	+	+	+

Hinweis:

1. Benötigt mindestens Firmware Version 4.00.100
2. Sollten Sie über ein nicht aufgeführtes Modell des Herstellers verfügen, so konsultieren Sie bitte die technische Dokumentation des Thin-Clients ob der gewünschte Chipkartenleser unterstützt wird.

Hersteller VLX							
Modell	pinpad 2.0	pinpad(a) 3.0	e-com 2.0	e-com(a) 3.0	secoder	e-com +	e-com (f)
Itona TC4300	-	+	-	+	+	+	+
Itona TC7335	-	+	-	+	+	+	+

Hinweis:

1. Es wird eLux RL (Linux-Kernel 2.6) benötigt

2. Zur Unterstützung der Reiner SCT-Chipkartenleser wurde aktuell ein device handler in eLux RL integriert. Die eLux RL-Version mit dieser Funktionalität wird ab Oktober 2009 im myelux.com-Portal zur Verfügung gestellt.
   Registrierte Benutzer werden gesondert informiert.

3. Unter eLux NG (Linux-Kernel 2.4) wird ausschließlich der pinpad (a) 3.0 (PID:0x300) unterstützt. Ein Update von eLux NG auf eLux RL ist ab Scout Version 11 möglich.

4. Sollten Sie über ein nicht aufgeführtes Modell des Herstellers verfügen, so konsultieren Sie bitte die technische Dokumentation des Thin-Clients ob der gewünschte Chipkartenleser unterstützt wird.

V2.0.0

11 Technische Referenzen

11.1 LED-Funktionen

Folgende Zustände der Leuchtdioden (LEDs) sind möglich:

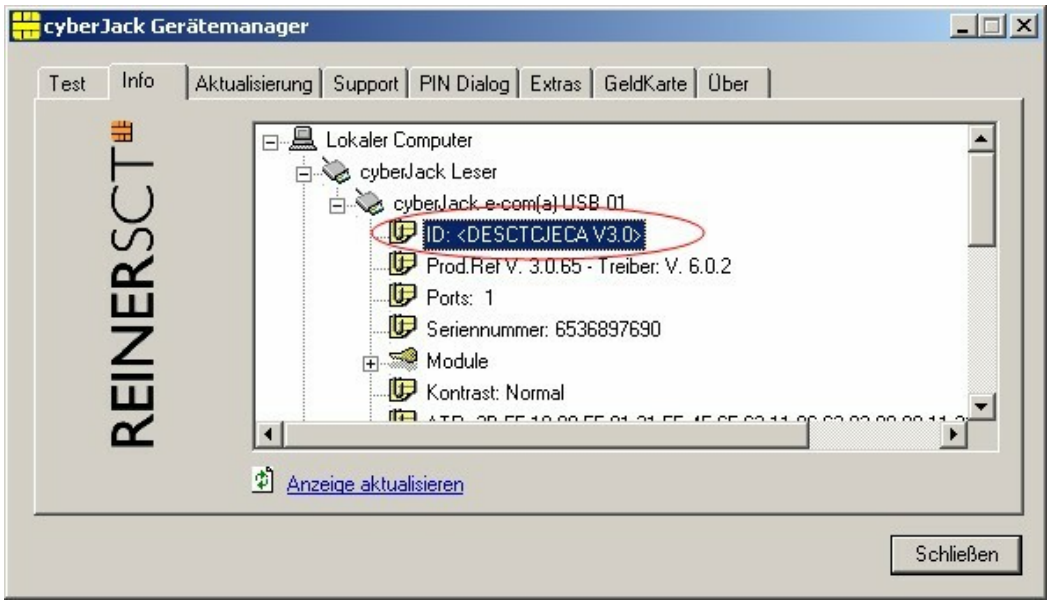
Grün	Gelb	Bedeutung
aus	beliebig	Karte ist abgeschaltet
blinkt	beliebig	Es hat in den letzten 3 Sekunden eine Kartenkommunikation stattgefunden
an	beliebig	Karte ist angeschaltet. In den letzten 3 Sekunden hat keine Kartenkommunikation stattgefunden.
beliebig	blinkt gleichmäßig periodisch	Modus sichere PIN-Eingabe. Es wird garantiert, dass keine Information über numerische Werte an den PC gesendet werden und das Display authentische (nicht vom PC übergebene) Texte anzeigt.
beliebig	blinkt periodisch: lang-kurz-kurz	Modus sichere PIN-Eingabe (Textanzeige vom PC). Es wird garantiert, dass keine Information über numerische Werte an den PC gesendet werden. Die Authentizität des angezeigten Textes kann nicht garantiert werden (der Text wurde innerhalb des Kommandos vom PC generiert).
beliebig	aus	Keine Zusicherung bezüglich des angezeigten Textes und der Geheimhaltung von Tastatureingaben.
Beide LEDs blinken synchron gleichmäßig periodisch, keine Anzeige im Display		Der Chipkartenleser hat sich wegen eines Fehlverhaltens deaktiviert. Bitte stecken Sie den Chipkartenleser aus und nach ca. 3 Sekunden wieder an. Sollte der Fehler weiterhin bestehen, dann wenden Sie sich bitte unter support@reiner-sct.com an unseren Support.

Hinweis: Beim cyber***Jack***® **secoder** entfällt die grüne LED

11.2 Geräteidentifizierung

Geräteidentifizierung mittels Gerätemanager

Über die Registerkarte *Info* können Sie Ihren installierten Chipkartenleser jederzeit eindeutig identifizieren (z.B. zum Abgleich mit Zertifizierungsdokumenten). Sollten Sie Zweifel an der Authentizität Ihres Gerätes haben, können Sie sich diesbezüglich mit den folgenden Daten unter support@reiner-sct.com bei REINER SCT rückversichern.



Folgende Identifikationsmerkmale (ID) deklarieren die jeweiligen Chipkartenleserplattformen, die z.B. auch in Zertifizierungsdokumenten aufgeführt sind:

ID	Chipkartenleser Hardwareplattform
DESCTCJSEC V3.0	cyber***Jack***® **secoder** V3.0
DESCTCJECF V3.0	cyber***Jack***® **e-com** V3.0 F-Typ
DESCTCJECA V3.0	cyber***Jack***® **e-com** V3.0 A-Typ
DESCTCJECP V3.0	cyber***Jack***® **e-com** plus V3.0

Anzeige von Typ und Version im Display des Chipkartenlesers

Um Typ, Betriebssystemversion und die jeweils im Chipkartenleser geladenen Applikationen anzuzeigen, drücken Sie die "@"-Taste der Tastatur Ihres cyber***Jack***® Chipkartenlesers. Im Display des Chipkartenlesers werden nun die aktuelle Bezeichnung des Typs und der Betriebssystemversion sowie die geladenen Applikationen mit der jeweiligen Bezeichnung und Version angezeigt.

Bei absichtlich herbeigeführten oder aufgrund eines technischen Defekts entstehenden Störungen des cyber***Jack***® Chipkartenlesers erfolgt eine Neuinitialisierung des Speichers des cyber***Jack***® Chipkartenlesers. Die aktuelle Firmware-Version wird dem Benutzer, begleitet durch ein periodisches Blinken der gelben LED, im Rahmen der Einschaltsequenz oder durch Drücken der Taste „@“ authentisch angezeigt

11.3 Sicherheitsfunktionen

Sichere PIN-Eingabe

Die Sichere PIN-Eingabe ist eine der wichtigsten Sicherheitsfunktionen eines Chipkartenlesers ab der Sicherheitsklasse 2. Um sicherzustellen, dass die PIN nicht im Chipkartenleser gespeichert wird, wurde die Hard- und Software des Chipkartenlesers strengen sicherheitstechnischen Evaluierungen unterzogen. Um sicherzustellen, dass die PIN nicht in der eingesteckten Chipkarte gespeichert werden kann, werden innerhalb des Modus "Sichere PIN-Eingabe" nur Befehle an die Chipkarte weitergeleitet, die zu Authentisierungszwecken verwendet werden können.

Diese sind ausschließlich:

- VERIFY
- CHANGE REFERENCE DATA
- DISABLE VERIFICATION REQUIREMENT
- ENABLE VERIFICATION REQUIREMENT
- RESET RETRY COUNTER

alle anderen Befehle zur Chipkarte werden vom Chipkartenleser blockiert.

Sicherer Firmwaredownload

Es ist möglich den Chipkartenleser mit einer neuen Firmware zu versehen, diese kann zum Beispiel mittels CD-ROM, per E-Mail oder online von den Webseiten von REINER SCT bezogen werden. Um in den Chipkartenleser eine neue Firmware zu laden, wird als wichtige Sicherheitsfunktion die Überprüfung der Herkunft der Firmware durch den Chipkartenleser selbst durchgeführt. So akzeptiert der Chipkartenleser nur Firmware die mittels RSA-Verfahren von REINER SCT elektronsich signiert wurde. Der Chipkartenleser führt jeweils vor dem Aufbringen einer neuen Firmware eine Signaturprüfung durch. Ein Speichern einer nicht von REINER SCT elektronisch signierten Firmware im Chipkartenleser ist nicht möglich.

Nach erfolgter Aktivierung der neuen Firmware kann mittels der Registerkarte *Info* des Gerätemanagers die aktuelle Firmwareversion im Chipkartenleser angezeigt werden. Nach der Bezeichnung *Prod.Ref* wird die aktuelle Firmwareversion des Chipkartenlesers angezeigt.

12 Sicherheitshinweise

Sicherheit von Kleinkindern

Die Geräte und sein Zubehör können Kleinteile enthalten. Halten Sie diese außerhalb der Reichweite von kleinen Kindern.

Allgemeiner Sicherheitshinweis

Stecken Sie keine Fremdkörper in den Kartenschlitz. Werfen Sie das Gerät oder die Batterien keinesfalls ins Feuer.

Pflege und Wartung

Ihr Gerät wurde mit großer Sorgfalt entwickelt und hergestellt und sollte auch mit Sorgfalt behandelt werden. Die folgenden Empfehlungen sollen Ihnen helfen einen dauerhaften Betrieb Ihres cyber***Jack***® sicherzustellen:

- Verwenden Sie das Gerät nicht in staubigen oder schmutzigen Umgebungen oder bewahren Sie es dort auf. Die beweglichen Teile und elektronischen Komponenten können beschädigt werden.
- Bewahren Sie das Gerät nicht in heißen Umgebungen auf. Hohe Temperaturen können die Lebensdauer elektronischer Geräte verkürzen und bestimmte Kunststoffe verformen oder zum Schmelzen bringen.
- Bewahren Sie das Gerät nicht in kalten Umgebungen auf. Wenn das Gerät anschließend wieder zu seiner normalen Temperatur zurückkehrt, kann sich in seinem Inneren Feuchtigkeit bilden und die elektronischen Schaltungen beschädigen.
- Lassen Sie das Gerät nicht fallen, setzen Sie es keinen Schlägen oder Stößen aus und schütteln Sie es nicht. Durch eine grobe Behandlung können im Gerät befindliche elektronische Schaltungen und mechanische Feinteile Schaden nehmen.
- Verwenden Sie keine scharfen Chemikalien, Reinigungslösungen oder starke Reinigungsmittel zur Reinigung des Geräts.
- Malen Sie das Gerät nicht an. Durch die Farbe können die beweglichen Teile verkleben und so den ordnungsgemäßen Betrieb verhindern.
- Reinigen Sie das Display und das Gehäuse nur mit einem weichen, sauberen und trockenen Tuch.
- Wenn ein Gerät nicht ordnungsgemäß funktioniert, bringen Sie es zu Ihrem Institut oder zu Ihrem Fachhändler bei dem Sie es gekauft haben zurück.

Entsorgung alter Elektrogeräte

Dieses Symbol auf dem Produkt oder seiner Verpackung weist darauf hin, dass es nicht mit dem Hausmüll entsorgt werden darf. Geben Sie es stattdessen an einer Sammelstelle für Elektrogeräte ab, die das Produkt dem Recycling zuführt. Durch eine ordnungsgemäße Entsorgung dieses Produkts vermeiden Sie potenzielle Umwelt- und Gesundheitsschäden, die aus unsachgemäßer Entsorgung dieses Produktes erwachsen können. Das Recycling von Stoffen schont zudem die natürlichen Ressourcen. Ausführlichere Informationen zum Recycling dieses Produkts erhalten Sie von der zuständigen Stelle Ihrer Stadt bzw. Gemeinde oder vom Abfallentsorgungsunternehmen.

13 Konformitätserklärungen

13.1 cyberJack pinpad

© 2012 REINER Kartengeräte GmbH & Co. KG

REINERSCT

EG - KONFORMITÄTSERKLÄRUNG

CE

Die Firma: Reiner Kartengeräte GmbH & Co. KG
Goethestrasse 14
78120 Furtwangen

erklärt, in alleiniger Verantwortung, dass das Produkt:

cyber*Jack*® pinpad – Chipkartenleser für Homebanking und elektronische Signatur

(Bezeichnung, Typ oder Modell, Los-, Chargen- oder Seriennummer, möglichst Herkunft und Stückzahl)

auf das sich diese Erklärung bezieht, in Übereinstimmung mit den aufgeführten Richtlinien 2004/108/EG einschließlich aller zutreffenden Änderungen des Europäischen Parlamentes und des Rates vom 15. Dezember 2004 ist.
Zur Beurteilung des Erzeugnisses hinsichtlich elektromagnetischer Verträglichkeit wurden folgende Normen herangezogen:

EMV nach EMV-Labor-Nr.: ***2 030 036-000***

EN 55022 : 2006 + A1 : 2007 Klasse B

EN 61000-6-1 : 2007

EN 61000-6-3 : 2007

(Titel und/oder Nummer, sowie Ausgabedatum der Norm(en) oder der anderen normativen Dokumente)

Die oben genannte Firma hält darüber hinaus folgende Technische Dokumentation zur Einsicht bereit:

- vorschriftsmäßige Bedienanleitung
- Pläne
- Beschreibung der Maßnahmen zur Sicherstellung der Konformität
- Sonstige Technische Dokumentation, wie:
  Serviceanleitung

intern: *Beachtung des Reiner- Qualitätsmanagementhandbuchs*

Hinweis: *Die gesamte Technische CE - Dokumentation ist unter 2 030 040-000 archiviert.*

Klaus Bechtold
Geschäftsführer

Furtwangen, 17.07.2012
(Ort und Datum der Ausstellung)

(Name, Unterschrift u. Funktion des Unterzeichnenden)

REINER SCT PDM
PC-2030026-000-C KFT ÄM 8041
KONFORMITÄTSERKLÄRUNG cyberJack pinpad

13.2 cyberJack secoder

© 2012 REINER Kartengeräte GmbH & Co. KG

REINERSCT

EG - KONFORMITÄTSERKLÄRUNG

CE

Die Firma: Reiner Kartengeräte GmbH & Co. KG
Goethestrasse 14
78120 Furtwangen

erklärt, in alleiniger Verantwortung, dass das Produkt:

cyber*Jack*® Secoder– Chipkartenleser für Homebanking und elektronische Signatur

(Bezeichnung, Typ oder Modell, Los-, Chargen- oder Seriennummer, möglichst Herkunft und Stückzahl)

auf das sich diese Erklärung bezieht, in Übereinstimmung mit den aufgeführten Richtlinien 2004/108/EG einschließlich aller zutreffenden Änderungen des Europäischen Parlamentes und des Rates vom 15. Dezember 2004 ist.
Zur Beurteilung des Erzeugnisses hinsichtlich elektromagnetischer Verträglichkeit wurden folgende Normen herangezogen:

EMV nach Schuhwerk-EMV-Labor-Nr.: ***2009001019***

EN 55022 : 2006 + A1 : 2007 Klasse B

EN 61000-6-1 : 2007

EN 61000-6-3 : 2007

(Titel und/oder Nummer, sowie Ausgabedatum der Norm(en) oder der anderen normativen Dokumente)

Die oben genannte Firma hält darüber hinaus folgende Technische Dokumentation zur Einsicht bereit:

- vorschriftsmäßige Bedienanleitung
- Pläne
- Beschreibung der Maßnahmen zur Sicherstellung der Konformität
- Sonstige Technische Dokumentation, wie:
  Serviceanleitung

intern: *Beachtung des Reiner- Qualitätsmanagementhandbuchs*

Hinweis: *Die gesamte Technische CE - Dokumentation ist unter 2 714 036-000 archiviert.*

Klaus Bechtold

Furtwangen, 17.07.2012
(Ort und Datum der Ausstellung)

Klaus Bechtold
Geschäftsführer
(Name, Unterschrift u. Funktion des Unterzeichnenden)

REINER SCT PDM
PC-2 714 036-C KFT
KONFORMITÄTSERKLÄRUNG cyberJack Secoder

13.3 cyberJack ecom

© 2012 REINER Kartengeräte GmbH & Co. KG

REINERSCT

EG - KONFORMITÄTSERKLÄRUNG

CE

Die Firma: Reiner Kartengeräte GmbH & Co. KG
Goethestrasse 14
78120 Furtwangen

erklärt, in alleiniger Verantwortung, dass das Produkt (das gleiche Produkt wird unter zwei unterschiedlichen Produktnamen vertrieben):

cyber*Jack*® e-com / cyber*Jack*® biometric– Chipkartenleser für Homebanking und elektronische Signatur

(Bezeichnung, Typ oder Modell, Los-, Chargen- oder Seriennummer, möglichst Herkunft und Stückzahl)

auf das sich diese Erklärung bezieht, in Übereinstimmung mit den aufgeführten Richtlinien 2004/108/EG einschließlich aller zutreffenden Änderungen des Europäischen Parlamentes und des Rates vom 15. Dezember 2004 ist.
Zur Beurteilung des Erzeugnisses hinsichtlich elektromagnetischer Verträglichkeit wurden folgende Normen herangezogen:

*EMV nach EMV-Labor-Nr.: **2 050 036-000***

EN 55022 : 2006 + A1 : 2007 Klasse B

EN 61000-6-1 : 2007

EN 61000-6-3 : 2007

(Titel und/oder Nummer, sowie Ausgabedatum der Norm(en) oder der anderen normativen Dokumente)

Die oben genannte Firma hält darüber hinaus folgende Technische Dokumentation zur Einsicht bereit:

- vorschriftsmäßige Bedienanleitung
- Pläne
- Beschreibung der Maßnahmen zur Sicherstellung der Konformität
- Sonstige Technische Dokumentation, wie:
  Serviceanleitung

intern: *Beachtung des Reiner- Qualitätsmanagementhandbuchs*

Hinweis: *Die gesamte Technische CE - Dokumentation ist unter 2 050 040-000 archiviert.*

Klaus Bechtold

Furtwangen, 17.07.2012
(Ort und Datum der Ausstellung)

Klaus Bechtold
Geschäftsführer
(Name, Unterschrift u. Funktion des Unterzeichnenden)

REINER SCT PDM
PC-2050026-000-C KFT ÄM 8041
KONFORMITÄTSERKLÄRUNG cyberJack e-com

13.4 cyberJack e-com plus

© 2012 REINER Kartengeräte GmbH & Co. KG

REINERSCT

EG - KONFORMITÄTSERKLÄRUNG

CE

Die Firma: Reiner Kartengeräte GmbH & Co. KG
Goethestrasse 14
78120 Furtwangen

erklärt, in alleiniger Verantwortung, dass das Produkt:

cyber*Jack*® e-com plus – Chipkartenleser für Homebanking und elektronische Signatur

(Bezeichnung, Typ oder Modell, Los-, Chargen- oder Seriennummer, möglichst Herkunft und Stückzahl)

auf das sich diese Erklärung bezieht, in Übereinstimmung mit den aufgeführten Richtlinien 2004/108/EG einschließlich aller zutreffenden Änderungen des Europäischen Parlamentes und des Rates vom 15. Dezember 2004 ist.
Zur Beurteilung des Erzeugnisses hinsichtlich elektromagnetischer Verträglichkeit wurden folgende Normen herangezogen:

EMV nach EMV-Labor-Nr.: ***2009010001***

EN 55022 : 2006 + A1 : 2007 Klasse B

EN 61000-6-1 : 2007

EN 61000-6-3 : 2007

(Titel und/oder Nummer, sowie Ausgabedatum der Norm(en) oder der anderen normativen Dokumente)

Die oben genannte Firma hält darüber hinaus folgende Technische Dokumentation zur Einsicht bereit:

- vorschriftsmäßige Bedienanleitung
- Pläne
- Beschreibung der Maßnahmen zur Sicherstellung der Konformität
- Sonstige Technische Dokumentation, wie:
  Serviceanleitung

intern: *Beachtung des Reiner- Qualitätsmanagementhandbuchs*

Hinweis: *Die gesamte Technische CE - Dokumentation ist unter 2 717 036-000 archiviert.*

Klaus Bechtold
Geschäftsführer

Furtwangen, 17.07.2012
(Ort und Datum der Ausstellung)

(Name, Unterschrift u. Funktion des Unterzeichnenden)

REINER SCT PDM
PC-2 717 036-C KFT
KONFORMITÄTSERKLÄRUNG cyberJack e com plus

14 SigG-Bestätigungen

14.1 cyberJack secoder

Bestätigung

von Produkten für qualifizierte elektronische Signaturen gemäß §§ 15 Abs. 7 und 17 Abs. 4 Gesetz über Rahmenbedingungen für elektronische Signaturen und § 11 Abs. 3 Verordnung zur elektronischen Signatur

TÜV Informationstechnik GmbH
Unternehmensgruppe TÜV NORD
Zertifizierungsstelle
Langemarckstraße 20
45141 Essen

bestätigt hiermit gemäß
§ 15 Abs. 7 Satz 1 Signaturgesetz[1] sowie § 11 Abs. 3 Signaturverordnung[2], dass der

Chipkartenleser
cyber*Jack*® secoder, Version 3.0
der
REINER Kartengeräte GmbH & Co. KG

den nachstehend genannten Anforderungen des SigG und der SigV entspricht.

Die Dokumentation zu dieser Bestätigung ist unter der Nummer

TUVIT.93154.TE.09.2008

registriert.

Essen, 16.09.2008

Dr. Christoph Sutter
Leiter Zertifizierungsstelle

TÜV Informationstechnik GmbH ist, gemäß der Veröffentlichung im Bundesanzeiger Nr. 52 vom 17. März 1999, Seite 4142 und gemäß § 25 Abs. 3 SigG, zur Erteilung von Bestätigungen für Produkte für qualifizierte elektronische Signaturen gemäß § 15 Abs. 7 und § 17 Abs. 4 SigG ermächtigt.

---

[1] Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG) vom 16.05.2001 (BGBl. I S. 876) zuletzt geändert durch Artikel 4 des Gesetzes vom 26.02.2007 (BGBl. I S. 179)

[2] Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16.11.2001 (BGBl. I S. 3074) zuletzt geändert durch Artikel 2 Abs. 18 des Gesetzes vom 23.11.2007 (BGBl. I S. 2631)

Die Bestätigung zur Registrierungsnummer TUVIT.93154.TE.09.2008 besteht aus 4 Seiten.

Beschreibung des Produktes:

1 Handelsbezeichnung des Produktes und Lieferumfang:

Chipkartenleser cyber*Jack*® secoder Version 3.0[3]

Auslieferung und Lieferumfang:

Als fertig konfiguriertes Gerät in Transportverpackung mit versiegeltem Gehäuse und Handbuch (auf der cyberJack Installations-CD):

- Chipkartenleser cyber*Jack*® secoder Version 3.0 bestehend aus der Hardware mit der Kennung DESCTCJSEC V3.0 und dem Betriebssystem cyberJack OS, Version 3.0,
- Handbuch: cyber*Jack*® – Installations- und Bedienungsanleitung, Stand: 09/2008.

Die cyberJack Installations-CD enthält ferner das Programm Gerätemanager und Treiber für Windows 2000/XP/Vista, Linux und MacOS X, die nicht Gegenstand der Bestätigung sind.

Hersteller:
REINER Kartengeräte GmbH & Co. KG
Goethestraße 14
78120 Furtwangen

2 Funktionsbeschreibung

Bei dem Produkt cyber*Jack*® secoder Version 3.0 handelt es sich um einen Chipkartenleser, der Rechnern den Zugriff auf Chipkarten nach ISO 7180, ISO 7813 und ISO 7816 ermöglicht. Den cyber*Jack*® secoder gibt es entweder mit USB 2.0- oder RS232-Schnittstelle zum Anschluss an einen Host-Rechner (PC). Beide Anschlussvarianten sind ansonsten funktional identisch.

Der Chipkartenleser cyber*Jack*® secoder ermöglicht im Modus „Sichere PIN-Eingabe", Identifikationsdaten in Form einer numerischen PIN durch die integrierte Tastatur zu erfassen und an sichere Signaturerstellungseinheiten (SSEE) weiterzuleiten. Dabei ist gewährleistet, dass die PIN ausschließlich über die Kontaktierschnittstelle an die SSEE übertragen wird und nicht über die USB 2.0- oder RS232-Schnittstelle an den angeschlossenen PC. An den PC wird lediglich für jede eingegebene Ziffer ein Standard-Key-Info-Block (SKI-Block) übertragen, der keine Informationen über die eingegebene Ziffer enthält. Nach Übertragung der PIN an die SSEE oder Abbruch der Übertragung wird der RAM-Speicher des cyber*Jack*® secoder, der die PIN (oder Teile davon) enthält, überschrieben.

Der Modus „Sichere PIN-Eingabe" wird über die PC-Schnittstelle per Kommando aktiviert und dem Benutzer durch eine blinkende gelbe LED, entweder gleichmäßig periodisch oder periodisch lang-kurz-kurz (siehe auch Abschnitt 10.1 des Handbuchs), signalisiert.

[3] Im Folgenden kurz mit cyber*Jack*® secoder bezeichnet.

Der cyber*Jack*® secoder bietet die Möglichkeit eines gesicherten Updates der Firmware. Neue Firmware-Versionen sind nicht Gegenstand dieser Bestätigung, können aber zukünftig nach Überprüfung durch die Bestätigungsstelle in einen Nachtrag zu dieser Bestätigung oder in eine neue Bestätigung aufgenommen werden.

Der cyber*Jack*® secoder ist geeignet als Modul eines zu bestätigenden Produktes für qualifizierte elektronische Signaturen nach § 2 Nr. 13 SigG, im Folgenden kurz Anwendung genannt, Identifikationsdaten (PIN) zu erfassen und an sichere Signaturerstellungseinheiten (SSEE) nach § 2 Nr. 10 SigG weiterzuleiten, sowie Hashwerte von der Anwendung zur SSEE und Signaturen zurück zur Anwendung zu übermitteln. Die Anwendung selbst ist nicht Gegenstand dieser Bestätigung.

3 Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Der Chipkartenleser cyber*Jack*® secoder erfüllt die Anforderungen nach § 15 Abs. 2 Nr. 1a) (keine Preisgabe oder Speicherung der Identifikationsdaten) und Abs. 4 (Erkennbarkeit sicherheitstechnischer Veränderungen) SigV.

3.2 Einsatzbedingungen

Dies gilt unter der Voraussetzung, dass folgende Einsatzbedingungen gewährleistet sind:

a) Technische Einsatzumgebung

Der Chipkartenleser cyber*Jack*® secoder benötigt zum Betrieb die folgende technische Einsatzumgebung:

- Host-Rechner (PC) mit RS232-Schnittstelle (Stromversorgung über die Tastaturschnittstelle) oder USB 2.0-Schnittstelle (Stromversorgung über die USB-Schnittstelle).
- Vom Hersteller zur Verfügung gestellte Treibersoftware (nicht Gegenstand der Bestätigung).
- Sichere Signaturerstellungseinheit nach § 2 Nr. 10 SigG basierend auf einer Prozessorchipkarte mit dem Protokoll T=0 oder T=1 entsprechend ISO7816 oder EMV2000 mit Chipkartenbetriebssystem, das zur PIN-Behandlung nur standardisierte Kommandos (VERIFY (INS-Byte=20h; ISO/IEC 7816-4), CHANGE REFERENCE DATA (INS-Byte=24h; ISO/IEC 7816-8), ENABLE VERIFICATION REQUIREMENT (INS-Byte=28h; ISO/IEC 7816-8), DISABLE VERIFICATION REQUIREMENT (INS-Byte=26h; ISO/IEC 7816-8) oder RESET RETRY COUNTER (INS-Byte=2Ch; ISO/IEC 7816-8)) spezifikationsgemäß verwendet.
- Signaturanwendungskomponente gemäß § 2 Nr. 13 SigG, die zur korrekten Umschaltung der Chipkartenleser in den Modus zur sicheren PIN-Eingabe das jeweils benötigte, o. g. standardisierte Kommando spezifikationsgemäß nutzt und in die Kommandos an dem Chipkartenleser zum Verifizieren bzw. Modifizieren der PIN einbindet.

Eine Übertragung der Evaluationsergebnisse auf andere Plattformen ist nicht möglich, sondern erfordert ggf. eine Reevaluation. Der Chipkartenleser cyber*Jack*® secoder darf deshalb ausschließlich in der oben beschriebenen Hard- und Softwareumgebung eingesetzt werden.

b) Auslieferung und Inbetriebnahme

Der Chipkartenleser cyber*Jack*® secoder wird als fertig konfiguriertes Gerät mit der zugehörigen Installationsanleitung in Transportverpackung mit versiegeltem Gehäuse ausgeliefert. Bei Inbetriebnahme ist zunächst die Unversehrtheit des Siegels zu prüfen.

c) Nutzung des cyber*Jack*® secoder

Während des Betriebes sind die folgenden Bedingungen für den sachgemäßen Einsatz zu beachten:

- Betrieb nur in der vom Anwender gegen Manipulationsversuche geschützten Arbeitsumgebung.
- Die Geräteversiegelung ist regelmäßig auf Unversehrtheit zu überprüfen.
- Beim Einschalten des Chipkartenlesers oder durch Drücken der Taste „@“ wird die Versionsnummer des cyberJack OS angezeigt. Dabei blinkt die gelbe LED periodisch zur Signalisierung der authentischen Versionsanzeige „cyberJack OS, Version: 3.0“. Die Hardware-Kennung „DESCTCJSEC V3.0“ lässt sich mittels des mitgelieferten Gerätemanagers auslesen.
- Der Einsatz für die qualifizierte elektronische Signatur setzt die Nutzung einer Signaturanwendungskomponente gemäß § 2 Nr. 11 SigG voraus. Diese muss für den Einsatz des Chipkartenlesers cyber*Jack*® secoder unter Verwendung der sicheren Umschaltung des Nummernblocks für die Erfassung der Identifikationsdaten (PIN) und für die zu verwendende sichere Signaturerstellungseinheit (gemäß § 2 Nr. 10 SigG) bestätigt sein.
- Die Eingabe der PIN auf der Tastatur des Chipkartenlesers muss unbeobachtet erfolgen.

3.3 Algorithmen und zugehörige Parameter

Entfällt

3.4 Prüfstufe und Mechanismenstärke

Der Chipkartenleser cyber*Jack*® secoder wurden erfolgreich nach der Prüfstufe E2 der ITSEC evaluiert. Die eingesetzten Sicherheitsmechanismen erreichen die Stärke **hoch**

Ende der Bestätigung

14.2 cyberJack e-com

Bestätigung

von Produkten für qualifizierte elektronische Signaturen gemäß §§ 15 Abs. 7 und 17 Abs. 4 Gesetz über Rahmenbedingungen für elektronische Signaturen und § 11 Abs. 3 Verordnung zur elektronischen Signatur

TÜV Informationstechnik GmbH
Unternehmensgruppe TÜV NORD
Zertifizierungsstelle
Langemarckstraße 20
45141 Essen

bestätigt hiermit gemäß
§ 15 Abs. 7 Satz 1 Signaturgesetz[1] sowie § 11 Abs. 3 Signaturverordnung[2],
dass der

Chipkartenleser
***cyberJack*® e-com, Version 3.0**
der
REINER Kartengeräte GmbH & Co. KG

den nachstehend genannten Anforderungen des SigG und der SigV entspricht.

Die Dokumentation zu dieser Bestätigung ist unter der Nummer

TUVIT.93155.TE.09.2008

registriert.

Essen, 16.09.2008

Dr. Christoph Sutter
Leiter Zertifizierungsstelle

TÜV Informationstechnik GmbH ist, gemäß der Veröffentlichung im Bundesanzeiger Nr. 52 vom 17. März 1999, Seite 4142 und gemäß § 25 Abs. 3 SigG, zur Erteilung von Bestätigungen für Produkte für qualifizierte elektronische Signaturen gemäß § 15 Abs. 7 und § 17 Abs. 4 SigG ermächtigt.

---

[1] Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG) vom 16.05.2001 (BGBl. I S. 876) zuletzt geändert durch Artikel 4 des Gesetzes vom 26.02.2007 (BGBl. I S. 179)

[2] Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16.11.2001 (BGBl. I S. 3074) zuletzt geändert durch Artikel 2 Abs. 18 des Gesetzes vom 23.11.2007 (BGBl. I S. 2631)

Die Bestätigung zur Registrierungsnummer TUVIT.93155.TE.09.2008 besteht aus 4 Seiten.

Beschreibung des Produktes:

1 Handelsbezeichnung des Produktes und Lieferumfang:

Chipkartenleser *cyberJack*® e-com Version 3.0[3]

Auslieferung und Lieferumfang:

Als fertig konfiguriertes Gerät in Transportverpackung mit versiegeltem Gehäuse und Handbuch (auf der cyberJack Installations-CD):

- Chipkartenleser *cyberJack*® e-com Version 3.0 bestehend aus der Hardware mit der Kennung DESCTCJECF V3.0 oder DESCTCJECA V3.0[4] und dem Betriebssystem cyberJack OS, Version 3.0,
- Handbuch: cyber*Jack*® – Installations- und Bedienungsanleitung, Stand: 09/2008.

Die cyberJack Installations-CD enthält ferner das Programm Gerätemanager und Treiber für Windows 2000/XP/Vista, Linux und MacOS X, die nicht Gegenstand der Bestätigung sind.

Hersteller:
REINER Kartengeräte GmbH & Co. KG
Goethestraße 14
78120 Furtwangen

2 Funktionsbeschreibung

Bei dem Produkt *cyberJack*® e-com Version 3.0 handelt es sich um einen Chipkartenleser, der Rechnern den Zugriff auf Chipkarten nach ISO 7180, ISO 7813 und ISO 7816 ermöglicht. Den *cyberJack*® e-com gibt es entweder mit USB 2.0-, RS232- oder LPT-Schnittstelle zum Anschluss an einen Host-Rechner (PC). Alle drei Anschlussvarianten sind ansonsten funktional identisch.

Der Chipkartenleser *cyberJack*® e-com ermöglicht im Modus „Sichere PIN-Eingabe", Identifikationsdaten in Form einer numerischen PIN durch die integrierte Tastatur zu erfassen und an sichere Signaturerstellungseinheiten (SSEE) weiterzuleiten. Dabei ist gewährleistet, dass die PIN ausschließlich über die Kontaktierschnittstelle an die SSEE übertragen wird und nicht über die USB 2.0-, RS232- oder LPT-Schnittstelle an den angeschlossenen PC. An den PC wird lediglich für jede eingegebene Ziffer ein Standard-Key-Info-Block (SKI-Block) übertragen, der keine Informationen über die eingegebene Ziffer enthält. Nach Übertragung der PIN an die SSEE oder Abbruch der Übertragung wird der RAM-Speicher des *cyberJack*® e-com, der die PIN (oder Teile davon) enthält, überschrieben.

Der Modus „Sichere PIN-Eingabe" wird über die PC-Schnittstelle per Kommando aktiviert und dem Benutzer durch eine blinkende gelbe LED, entweder gleichmäßig periodisch oder periodisch lang-kurz-kurz (siehe auch Abschnitt 10.1 des Handbuchs), signalisiert.

---

[3] Im Folgenden kurz mit *cyberJack*® e-com bezeichnet.
[4] Die beiden Kennungen kennzeichnen zwei Hardwarevarianten des cyberJack® e-com, im Handbuch als F-Typ und A-Typ bezeichnet, die sich funktional gleich verhalten.

Der *cyberJack*® e-com bietet die Möglichkeit eines gesicherten Updates der Firmware. Neue Firmware-Versionen sind nicht Gegenstand dieser Bestätigung, können aber zukünftig nach Überprüfung durch die Bestätigungsstelle in einen Nachtrag zu dieser Bestätigung oder in eine neue Bestätigung aufgenommen werden.

Der *cyberJack*® e-com ist geeignet als Modul eines zu bestätigenden Produktes für qualifizierte elektronische Signaturen nach § 2 Nr. 13 SigG, im Folgenden kurz Anwendung genannt, Identifikationsdaten (PIN) zu erfassen und an sichere Signaturerstellungseinheiten (SSEE) nach § 2 Nr. 10 SigG weiterzuleiten, sowie Hashwerte von der Anwendung zur SSEE und Signaturen zurück zur Anwendung zu übermitteln. Die Anwendung selbst ist nicht Gegenstand dieser Bestätigung.

3 Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Der Chipkartenleser *cyberJack*® e-com erfüllt die Anforderungen nach § 15 Abs. 2 Nr. 1a) (keine Preisgabe oder Speicherung der Identifikationsdaten) und Abs. 4 (Erkennbarkeit sicherheitstechnischer Veränderungen) SigV.

3.2 Einsatzbedingungen

Dies gilt unter der Voraussetzung, dass folgende Einsatzbedingungen gewährleistet sind:

a) Technische Einsatzumgebung

Der Chipkartenleser *cyberJack*® e-com benötigt zum Betrieb die folgende technische Einsatzumgebung:

- Host-Rechner (PC) mit RS232-Schnittstelle (Stromversorgung über die Tastaturschnittstelle), LPT-Schnittstelle (Stromversorgung über die Tastaturschnittstelle) oder USB 2.0-Schnittstelle (Stromversorgung über die USB 2.0-Schnittstelle).
- Vom Hersteller zur Verfügung gestellte Treibersoftware (nicht Gegenstand der Bestätigung).
- Sichere Signaturerstellungseinheit nach § 2 Nr. 10 SigG basierend auf einer Prozessorchipkarte mit dem Protokoll T=0 oder T=1 entsprechend ISO7816 oder EMV2000 mit Chipkartenbetriebssystem, das zur PIN-Behandlung nur standardisierte Kommandos (VERIFY (INS-Byte=20h; ISO/IEC 7816-4), CHANGE REFERENCE DATA (INS-Byte=24h; ISO/IEC 7816-8), ENABLE VERIFICATION REQUIREMENT (INS-Byte=28h; ISO/IEC 7816-8), DISABLE VERIFICATION REQUIREMENT (INS-Byte=26h; ISO/IEC 7816-8) oder RESET RETRY COUNTER (INS-Byte=2Ch; ISO/IEC 7816-8)) spezifikationsgemäß verwendet.
- Signaturanwendungskomponente gemäß § 2 Nr. 13 SigG, die zur korrekten Umschaltung der Chipkartenleser in den Modus zur sicheren PIN-Eingabe das jeweils benötigte, o. g. standardisierte Kommando spezifikationsgemäß nutzt

und in die Kommandos an den Chipkartenleser zum Verifizieren bzw. Modifizieren der PIN einbindet.

Eine Übertragung der Evaluationsergebnisse auf andere Plattformen ist nicht möglich, sondern erfordert ggf. eine Reevaluation. Der Chipkartenleser *cyberJack*® e-com darf deshalb ausschließlich in der oben beschriebenen Hard- und Softwareumgebung eingesetzt werden.

b) Auslieferung und Inbetriebnahme

Der Chipkartenleser *cyberJack*® e-com wird als fertig konfiguriertes Gerät mit der zugehörigen Installationsanleitung in Transportverpackung mit versiegeltem Gehäuse ausgeliefert. Bei Inbetriebnahme ist zunächst die Unversehrtheit des Siegels zu prüfen.

c) Nutzung des *cyberJack*® e-com

Während des Betriebes sind die folgenden Bedingungen für den sachgemäßen Einsatz zu beachten:

- Betrieb nur in der vom Anwender gegen Manipulationsversuche geschützten Arbeitsumgebung.
- Die Geräteversiegelung ist regelmäßig auf Unversehrtheit zu überprüfen.
- Beim Einschalten des Chipkartenlesers oder durch Drücken der Taste „@“ wird die Versionsnummer des cyberJack OS angezeigt. Dabei blinkt die gelbe LED periodisch zur Signalisierung der authentischen Versionsanzeige „cyberJack OS, Version: 3.0“. Die Hardware-Kennung „DESCTCJECF V3.0 oder DESCTCJECA V3.0“ lässt sich mittels des mitgelieferten Gerätemanagers auslesen.
- Der Einsatz für die qualifizierte elektronische Signatur setzt die Nutzung einer Signaturanwendungskomponente gemäß § 2 Nr. 11 SigG voraus. Diese muss für den Einsatz des Chipkartenlesers *cyberJack*® e-com unter Verwendung der sicheren Umschaltung des Nummernblocks für die Erfassung der Identifikationsdaten (PIN) und für die zu verwendende sichere Signaturerstellungseinheit (gemäß § 2 Nr. 10 SigG) bestätigt sein.
- Die Eingabe der PIN auf der Tastatur des Chipkartenlesers muss unbeobachtet erfolgen.

3.3 Algorithmen und zugehörige Parameter

Entfällt

3.4 Prüfstufe und Mechanismenstärke

Der Chipkartenleser *cyberJack*® e-com wurden erfolgreich nach der Prüfstufe E2 der ITSEC evaluiert. Die eingesetzten Sicherheitsmechanismen erreichen die Stärke **hoch**

Ende der Bestätigung

14.3 cyberJack e-com plus

Bestätigung

von Produkten für qualifizierte elektronische Signaturen gemäß §§ 15 Abs. 7 und 17 Abs. 4 Gesetz über Rahmenbedingungen für elektronische Signaturen und § 11 Abs. 3 Verordnung zur elektronischen Signatur

TÜV Informationstechnik GmbH
Unternehmensgruppe TÜV NORD
Zertifizierungsstelle
Langemarckstraße 20
45141 Essen

bestätigt hiermit gemäß
§ 15 Abs. 7 Satz 1 Signaturgesetz[1] sowie § 11 Abs. 3 Signaturverordnung[2],
dass der

Chipkartenleser
***cyberJack*® e-com plus, Version 3.0**
der
REINER Kartengeräte GmbH & Co. KG

den nachstehend genannten Anforderungen des SigG und der SigV entspricht.

Die Dokumentation zu dieser Bestätigung ist unter der Nummer

TUVIT.93156.TE.09.2008

registriert.

Essen, 16.09.2008

Dr. Christoph Sutter
Leiter Zertifizierungsstelle

TÜV Informationstechnik GmbH ist, gemäß der Veröffentlichung im Bundesanzeiger Nr. 52 vom 17. März 1999, Seite 4142 und gemäß § 25 Abs. 3 SigG, zur Erteilung von Bestätigungen für Produkte für qualifizierte elektronische Signaturen gemäß § 15 Abs. 7 und § 17 Abs. 4 SigG ermächtigt.

---

[1] Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG) vom 16.05.2001 (BGBl. I S. 876) zuletzt geändert durch Artikel 4 des Gesetzes vom 26.02.2007 (BGBl. I S. 179)

[2] Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16.11.2001 (BGBl. I S. 3074) zuletzt geändert durch Artikel 2 Abs. 18 des Gesetzes vom 23.11.2007 (BGBl. I S. 2631)

Die Bestätigung zur Registrierungsnummer TUVIT.93156.TE.09.2008 besteht aus 4 Seiten.

Beschreibung des Produktes:

1 Handelsbezeichnung des Produktes und Lieferumfang:

Chipkartenleser *cyberJack*® e-com plus Version 3.0[3]

Auslieferung und Lieferumfang:

Als fertig konfiguriertes Gerät in Transportverpackung mit versiegeltem Gehäuse und Handbuch (auf der cyberJack Installations-CD):

- Chipkartenleser *cyberJack*® e-com plus Version 3.0 bestehend aus der Hardware mit der Kennung DESCTCJECP V3.0 und dem Betriebssystem cyberJack OS, Version 3.0,
- Handbuch: cyber*Jack*® – Installations- und Bedienungsanleitung, Stand: 09/2008.

Die cyberJack Installations-CD enthält ferner das Programm Gerätemanager und Treiber für Windows 2000/XP/Vista, Linux und MacOS X, die nicht Gegenstand der Bestätigung sind.

Hersteller:
REINER Kartengeräte GmbH & Co. KG
Goethestraße 14
78120 Furtwangen

2 Funktionsbeschreibung

Bei dem Produkt *cyberJack*® e-com plus Version 3.0 handelt es sich um einen Chipkartenleser, der Rechnern den Zugriff auf Chipkarten nach ISO 7180, ISO 7813 und ISO 7816 ermöglicht. Den *cyberJack*® e-com plus gibt es entweder mit USB 2.0- oder RS232-Schnittstelle zum Anschluss an einen Host-Rechner (PC). Alle drei Anschlussvarianten sind ansonsten funktional identisch.

Der Chipkartenleser *cyberJack*® e-com plus ermöglicht im Modus „Sichere PIN-Eingabe", Identifikationsdaten in Form einer numerischen PIN durch die integrierte Tastatur zu erfassen und an sichere Signaturerstellungseinheiten (SSEE) weiterzuleiten. Dabei ist gewährleistet, dass die PIN ausschließlich über die Kontaktierschnittstelle an die SSEE übertragen wird und nicht über die USB 2.0- oder RS232-Schnittstelle an den angeschlossenen PC. An den PC wird lediglich für jede eingegebene Ziffer ein Standard-Key-Info-Block (SKI-Block) übertragen, der keine Informationen über die eingegebene Ziffer enthält. Nach Übertragung der PIN an die SSEE oder Abbruch der Übertragung wird der RAM-Speicher des *cyberJack*® e-com plus, der die PIN (oder Teile davon) enthält, überschrieben.

Der Modus „Sichere PIN-Eingabe" wird über die PC-Schnittstelle per Kommando aktiviert und dem Benutzer durch eine blinkende gelbe LED, entweder gleichmäßig periodisch oder periodisch lang-kurz-kurz (siehe auch Abschnitt 10.1 des Handbuchs), signalisiert.

[3] Im Folgenden kurz mit cyberJack® e-com plus bezeichnet.

Der *cyberJack*® e-com plus bietet die Möglichkeit eines gesicherten Updates der Firmware. Neue Firmware-Versionen sind nicht Gegenstand dieser Bestätigung, können aber zukünftig nach Überprüfung durch die Bestätigungsstelle in einen Nachtrag zu dieser Bestätigung oder in eine neue Bestätigung aufgenommen werden.

Der *cyberJack*® e-com plus ist geeignet als Modul eines zu bestätigenden Produktes für qualifizierte elektronische Signaturen nach § 2 Nr. 13 SigG, im Folgenden kurz Anwendung genannt, Identifikationsdaten (PIN) zu erfassen und an sichere Signaturerstellungseinheiten (SSEE) nach § 2 Nr. 10 SigG weiterzuleiten, sowie Hashwerte von der Anwendung zur SSEE und Signaturen zurück zur Anwendung zu übermitteln. Die Anwendung selbst ist nicht Gegenstand dieser Bestätigung.

3 Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Der Chipkartenleser *cyberJack*® e-com plus erfüllt die Anforderungen nach § 15 Abs. 2 Nr. 1a) (keine Preisgabe oder Speicherung der Identifikationsdaten) und Abs. 4 (Erkennbarkeit sicherheitstechnischer Veränderungen) SigV.

3.2 Einsatzbedingungen

Dies gilt unter der Voraussetzung, dass folgende Einsatzbedingungen gewährleistet sind:

a) Technische Einsatzumgebung

Der Chipkartenleser *cyberJack*® e-com plus benötigt zum Betrieb die folgende technische Einsatzumgebung:

- Host-Rechner (PC) mit RS232-Schnittstelle (Stromversorgung über die Tastaturschnittstelle) oder USB 2.0-Schnittstelle (Stromversorgung über die USB-Schnittstelle).
- Vom Hersteller zur Verfügung gestellte Treibersoftware (nicht Gegenstand der Bestätigung).
- Sichere Signaturerstellungseinheit nach § 2 Nr. 10 SigG basierend auf einer Prozessorchipkarte mit dem Protokoll T=0 oder T=1 entsprechend ISO7816 oder EMV2000 mit Chipkartenbetriebssystem, das zur PIN-Behandlung nur standardisierte Kommandos (VERIFY (INS-Byte=20h; ISO/IEC 7816-4), CHANGE REFERENCE DATA (INS-Byte=24h; ISO/IEC 7816-8), ENABLE VERIFICATION REQUIREMENT (INS-Byte=28h; ISO/IEC 7816-8), DISABLE VERIFICATION REQUIREMENT (INS-Byte=26h; ISO/IEC 7816-8) oder RESET RETRY COUNTER (INS-Byte=2Ch; ISO/IEC 7816-8)) spezifikationsgemäß verwendet.
- Signaturanwendungskomponente gemäß § 2 Nr. 13 SigG, die zur korrekten Umschaltung der Chipkartenleser in den Modus zur sicheren PIN-Eingabe das jeweils benötigte, o. g. standardisierte Kommando spezifikationsgemäß nutzt

und in die Kommandos an den Chipkartenleser zum Verifizieren bzw. Modifizieren der PIN einbindet.

Eine Übertragung der Evaluationsergebnisse auf andere Plattformen ist nicht möglich, sondern erfordert ggf. eine Reevaluation. Der Chipkartenleser *cyberJack*® e-com plus darf deshalb ausschließlich in der oben beschriebenen Hard- und Softwareumgebung eingesetzt werden.

b) Auslieferung und Inbetriebnahme

Der Chipkartenleser *cyberJack*® e-com plus wird als fertig konfiguriertes Gerät mit der zugehörigen Installationsanleitung in Transportverpackung mit versiegeltem Gehäuse ausgeliefert. Bei Inbetriebnahme ist zunächst die Unversehrtheit des Siegels zu prüfen.

c) Nutzung des cyberJack® e-com plus

Während des Betriebes sind die folgenden Bedingungen für den sachgemäßen Einsatz zu beachten:

- Betrieb nur in der vom Anwender gegen Manipulationsversuche geschützten Arbeitsumgebung.
- Die Geräteversiegelung ist regelmäßig auf Unversehrtheit zu überprüfen.
- Beim Einschalten des Chipkartenlesers oder durch Drücken der Taste „@“ wird die Versionsnummer des cyberJack OS angezeigt. Dabei blinkt die gelbe LED periodisch zur Signalisierung der authentischen Versionsanzeige „cyberJack OS, Version: 3.0“. Die Hardware-Kennung „DESCTCJECP V3.0“ lässt sich mittels des mitgelieferten Gerätemanagers auslesen.
- Der Einsatz für die qualifizierte elektronische Signatur setzt die Nutzung einer Signaturanwendungskomponente gemäß § 2 Nr. 11 SigG voraus. Diese muss für den Einsatz des Chipkartenlesers *cyberJack*® e-com plus unter Verwendung der sicheren Umschaltung des Nummernblocks für die Erfassung der Identifikationsdaten (PIN) und für die zu verwendende sichere Signaturerstellungseinheit (gemäß § 2 Nr. 10 SigG) bestätigt sein.
- Die Eingabe der PIN auf der Tastatur des Chipkartenlesers muss unbeobachtet erfolgen.

3.3 Algorithmen und zugehörige Parameter

Entfällt

3.4 Prüfstufe und Mechanismenstärke

Der Chipkartenleser *cyberJack*® e-com plus wurden erfolgreich nach der Prüfstufe E2 der ITSEC evaluiert. Die eingesetzten Sicherheitsmechanismen erreichen die Stärke **hoch**

Ende der Bestätigung

Index

- A -

ATC 18

- B -

Bedienelemente
- Display 6
- Leuchtdioden 6
- Tastatur 6

- C -

CITRIX 28

cyberJack
- biometric 2
- e-com 2
- e-com plus 2
- pinpad 2
- secoder 2

cyberJack biometric 22

- G -

Gerätemanager 13

Gerätesiegel 5

- H -

HHD 1.3 18

- I -

Installation
- Softwarekomponente 11

- K -

Konformitätserklärung
- cyberJack e-com 42
- cyberJack e-com plus 43
- cyberJack pinpad 40
- cyberJack secoder 41

- L -

LED-Funktion 36

LPT 10

- M -

Modulverwaltung 21

- S -

Seriell 9

Sichere PIN-Eingabe 7, 17

Sicheres Ändern der PIN 17

Sicherheitshinweise 39

SigG-Bestätigungen
- cyberJack e-com 48
- cyberJack e-com plus 52
- cyberJack secoder 44

Standfuß 5

Support
- Gewährleistung 27
- Service 27

- T -

TAN 18

TAN-Erzeugung 18

TWIN 9

- U -

USB-Anschluss 8

- W -

Windows Terminal Server 28

Stand: 01-2013

Reiner Kartengeräte GmbH & Co.KG

Goethestrasse 14
78120 Furtwangen
Germany
Telefon: +49 (0)7723 5056-0
Telefax: +49 (0)7723 5056-78
E-Mail: sales@reiner-sct.com
Internet: www.reiner-sct.com